



Benutzerhandbuch

AWS Security Hub



AWS Security Hub : Benutzerhandbuch

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

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

Table of Contents

Was ist AWS Security Hub?	1
Features	1
Integrationen	2
AWS-Regionen wird für die öffentliche Vorschau unterstützt	2
Zugriffsmöglichkeiten	4
Preisgestaltung	4
Erste Schritte	5
Security Hub aktivieren	5
Empfehlungen	15
Konzepte	17
OCSF-Ergebnisse	18
Ergebnisse der Berichterstattung	18
Deckungsergebnisse für Security Hub CSPM	19
Ergebnisse der Berichterstattung für GuardDuty	19
Ergebnisse der Berichterstattung für Amazon Inspector	20
Ergebnisse der Berichterstattung für Macie	20
Feststellungen zur Exposition	20
Unterstützte Ressourcen	21
Unterstützte Eigenschaften	21
Generierung von Ergebnissen zur Gefährdung	23
Bestimmung des Schweregrads eines Expositionsergebnisses	28
Überprüfung der Ergebnisse zur Exposition	28
Behebung von Risikoprüfungen	31
Ergebnisse der Angriffssequenz	95
Überprüfung der Ergebnisse zur Angriffssequenz	95
Behebung von Ergebnissen der Angriffssequenz	96
Regeln für die Automatisierung	97
Wichtigste Verbesserungen	98
Externe Integration	98
Von OCSF unterstützte Kriterien	98
OCSF-Felder für die AutomationRulesFindingFieldsUpdate	98
Integrationen von Drittanbietern	99
Erstellen Sie einen KMS-Schlüssel	99
Jira Cloud	102

ServiceNow	107
Dashboard	111
Das Widget mit der Zusammenfassung des Risikos	112
Das Widget mit der Zusammenfassung der Bedrohungen	112
Das Widget „Sicherheitsabdeckung“	113
Details zu Ressourcen in Security Hub anzeigen	113
Diagramm mit potenziellem Angriffspfad	115
Security Hub deaktivieren	115
Was ist AWS Security Hub CSPM?	117
Vorteile von Security Hub CSPM	118
Zugreifen auf Security Hub CSPM	119
Zugehörige Services	120
Kostenlose Testversion, Nutzung und Preisgestaltung von Security Hub CSPM	121
Anzeigen von Nutzungsdetails und geschätzten Kosten	121
Preisdetails	122
Security Hub CSPM-Konzepte	123
Security Hub CSPM aktivieren	130
Überprüfung der erforderlichen Berechtigungen	130
Aktivierung von Security Hub CSPM mit Unternehmensintegration	130
Zentrale Konfiguration	131
Manuelles Aktivieren von Security Hub CSPM	132
Skript zur Aktivierung mehrerer Konten	134
Nächste Schritte: Posture-Management und Integrationen	135
Konfiguration AWS Config für Security Hub CSPM	135
Überlegungen vor der Aktivierung und Konfiguration AWS Config	136
Ressourcen aufzeichnen in AWS Config	137
Möglichkeiten zur Aktivierung und Konfiguration AWS Config	138
Config.1-Steuerung	139
Generierung der serviceverknüpften Regeln	140
Kostenüberlegungen	140
Lokale Konfiguration	141
Zentrale Konfiguration	142
Vorteile der Verwendung der zentralen Konfiguration	143
Wann sollte die zentrale Konfiguration verwendet werden?	144
Zentrale Begriffe und Konzepte zur Konfiguration	144
Aktivierung der zentralen Konfiguration	151

Zentral verwaltet versus selbstverwaltet	156
Wie funktionieren Konfigurationsrichtlinien	161
Konfigurationsrichtlinien erstellen und zuordnen	167
Überprüfung des Status und der Einzelheiten der Konfigurationsrichtlinien	174
Aktualisierung der Konfigurationsrichtlinien	178
Löschen von Konfigurationsrichtlinien	183
Aufheben der Zuordnung einer Konfiguration	186
Konfiguration im Kontext	188
Deaktivierung der zentralen Konfiguration	190
Security Hub CSPM für mehrere Konten verwalten	194
Konten verwalten mit AWS Organizations	194
Manuelles Verwalten von Konten auf Einladung	195
Empfehlungen für Umgebungen mit mehreren Konten	196
Maximale Anzahl von Mitgliedern pro Konto	196
Beziehungen zwischen Administrator und Mitglied erstellen	196
Koordination der Administratorkonten für alle Dienste	197
Konten verwalten mit AWS Organizations	198
Integration mit AWS Organizations	200
Automatisches Aktivieren von Security Hub CSPM in neuen Konten	209
Manuelles Aktivieren von Security Hub CSPM in neuen Konten	211
Aufheben der Zuordnung von Mitgliedskonten der Organisation	214
Verwalten von Konten auf Einladung	216
Mitgliedskonten hinzufügen und einladen	217
Auf eine Einladung antworten	221
Aufheben der Zuordnung von Mitgliedskonten	224
Mitgliedskonten löschen	226
Trennung von einem Administratorkonto	227
Übergang zu AWS Organizations	229
Zulässige Aktionen von Administrator- und Mitgliedskonten	230
Auswirkung von Kontoaktionen auf CSPM-Daten	237
Security Hub CSPM ist deaktiviert	237
Das Mitgliedskonto wurde vom Administratorkonto getrennt	238
Das Mitgliedskonto wurde aus einer Organisation entfernt	238
Das Konto ist gesperrt	239
Das Konto ist geschlossen	239
Aggregation von CSPM-Daten über Regionen hinweg	241

Arten von Daten, die aggregiert sind	242
Aggregation für Administrator- und Mitgliedskonten	244
Zentrale Konfiguration und Aggregation	245
Aggregation aktivieren	246
Überprüfung der Aggregationseinstellungen	248
Aktualisierung der Aggregationseinstellungen	250
Die Aggregation wird beendet	252
Der Suchaggregator (Konsole) wird gelöscht	252
CSPM-Standards	254
Referenz zu Standards	255
AWS Bewährte grundlegende Sicherheitsmethoden	257
AWS Kennzeichnung von Ressourcen	276
Benchmark für die Stiftungen AWS	282
NIST SP 800-53 Version 5	301
NIST SP 800-171 Revision 2	319
PCI DSS	325
Vom Service verwaltete Standards	336
Einen Standard aktivieren	350
Aktivierung eines Standards in mehreren Konten und AWS-Regionen	351
Aktivierung eines Standards in einem einzigen Konto und AWS-Region	352
Den Status eines Standards überprüfen	354
Überprüfung der Einzelheiten eines Standards	357
Grundlegendes zur Standard-Sicherheitsbewertung	358
Überprüfung der Kontrollen im Hinblick auf einen Standard	359
Automatisch aktivierte Standards ausschalten	361
Deaktivierung eines Standards	362
Deaktivierung eines Standards in mehreren Konten und AWS-Regionen	363
Deaktivierung eines Standards in einem einzelnen Konto und AWS-Region	364
CSPM-Steuerelemente	366
Ansicht „Konsolidierte Kontrollen“	366
Zusammenfassung der Sicherheitsbewertung für Kontrollen	367
Referenz zu Steuerelementen	368
Änderungsprotokoll für Steuerelemente	504
AWS-Konto steuert	587
AWS Amplify steuert	588
Amazon API Gateway Gateway-Management	592

AWS AppConfig steuert	598
AppFlow Amazon-Kontrollen	605
AWS App Runner steuert	607
AWS AppSync steuert	610
Amazon Athena Athena-Steuerung	615
AWS Backup steuert	620
AWS Batch steuert	629
AWS Certificate Manager steuert	636
AWS CloudFormation steuert	640
CloudFront Amazon-Kontrollen	643
AWS CloudTrail steuert	655
CloudWatch Amazon-Kontrollen	667
AWS CodeArtifact steuert	715
AWS CodeBuild steuert	716
Amazon CodeGuru Profiler-Steuerelemente	723
Kontrollen von Amazon CodeGuru Reviewer	724
Amazon Cognito-Steuerelemente	726
AWS Config steuert	728
Amazon Connect Connect-Steuerelemente	732
Amazon Data Firehose-Steuerelemente	734
AWS DataSync steuert	735
Amazon Detective steuert	738
AWS DMS steuert	739
Amazon DocumentDB-Steuerelemente	754
Amazon DynamoDB-Steuerelemente	760
EC2 Amazon-Kontrollen	768
Amazon EC2 Auto Scaling-Steuerelemente	851
Amazon ECR-Steuerelemente	860
Amazon ECS-Steuerelemente	866
Amazon EFS-Steuerelemente	881
Amazon EKS-Steuerelemente	888
ElastiCache Amazon-Kontrollen	895
AWS Elastic Beanstalk Kontrollen	901
Elastic Load Balancing Balancing-Steuerelemente	905
Elasticsearch-Steuerelemente	922
Amazon EMR-Steuerelemente	931

EventBridge Amazon-Kontrollen	936
Kontrollen von Amazon Fraud Detector	939
FSx Amazon-Kontrollen	947
AWS Global Accelerator Kontrollen	952
AWS Glue steuert	954
GuardDuty Amazon-Kontrollen	958
AWS Identity and Access Management steuert	972
Amazon Inspector-Steuerelemente	1010
AWS IoT steuert	1015
AWS Steuerung von IoT Events	1025
AWS SiteWise IoT-Steuerungen	1030
AWS TwinMaker IoT-Steuerungen	1038
AWS IoT Wireless IoT-Steuerungen	1045
Amazon IVS Kontrollen	1050
Amazon Keyspaces-Steuerelemente	1055
Amazon Kinesis Kinesis-Steuerung	1057
AWS KMS steuert	1061
AWS Lambda steuert	1067
Amazon Macie-Steuerelemente	1074
Amazon MSK-Steuerungen	1076
Amazon MQ-Steuerelemente	1082
Amazon Neptune Neptune-Steuerungen	1087
AWS Network Firewall steuert	1095
Amazon OpenSearch Service-Kontrollen	1105
AWS Private CA steuert	1116
Amazon RDS-Steuerelemente	1119
Amazon Redshift Redshift-Steuerelemente	1167
Steuerelemente von Amazon Redshift Serverless	1185
Amazon Route 53-Steuerelemente	1193
Amazon S3 S3-Steuerelemente	1196
Amazon SageMaker KI-Steuerungen	1222
AWS Secrets Manager Steuerungen	1231
AWS Service Catalog steuert	1238
Steuerelemente von Amazon Simple Email Service	1239
Amazon SNS SNS-Steuerelemente	1242
Amazon SQS-Steuerelemente	1247

AWS Step Functions Steuerungen	1251
AWS Systems Manager Steuerungen	1254
AWS Transfer Family steuert	1262
AWS WAF steuert	1271
WorkSpaces Amazon-Kontrollen	1280
Berechtigungen zur Konfiguration von Steuerelementen	1281
Steuerungen aktivieren	1282
Aktivierung einer standardübergreifenden Steuerung	1283
Aktivierung einer Steuerung in einem bestimmten Standard	1286
Automatische Aktivierung neuer Steuerungen	1289
Steuerungen deaktivieren	1291
Ein standardübergreifendes Steuerelement deaktivieren	1293
Deaktivierung eines Steuerelements in einem bestimmten Standard	1296
Vorgeschlagene Steuerelemente zum Deaktivieren	1299
Sicherheitsüberprüfungen und Ergebnisse	1304
Erforderliche AWS Config Ressourcen für Kontrollbefunde	1305
Zeitplan für die Ausführung von Sicherheitsprüfungen	1357
Generierung und Aktualisierung von Kontrollbefunden	1359
Konformitätsstatus und Kontrollstatus	1377
Berechnung von Sicherheitswerten	1379
Kontrollkategorien	1382
Identifizieren	1382
Schutz	1383
Detect	1384
Reagieren	1385
Wiederherstellung	1385
Überprüfung der Einzelheiten der Kontrollen	1386
Details für ein Steuerelement anzeigen	1387
Steuerelemente zum Filtern und Sortieren	1389
Steuerparameter	1390
Auswirkung der Änderung von Steuerparameterwerten	1391
Steuerelemente, die benutzerdefinierte Parameter unterstützen	1393
Überprüfung der aktuellen Steuerparameterwerte	1393
Anpassen von Steuerparametern	1395
Rückkehr zu den Standardsteuerparametern	1400
Überprüfung des Status von Änderungen der Steuerparameter	1405

Überprüfung und Verwaltung der Kontrollergebnisse	1406
Filterung und Sortierung der Kontrollergebnisse	1406
Stichproben von Kontrollbefunden	1407
CSPM-Integrationen	1433
Überprüfung einer Liste von Integrationen	1434
Den Fluss von Erkenntnissen aus einer Integration ermöglichen	1435
Deaktivierung des Flusses von Erkenntnissen aus einer Integration	1437
Ergebnisse einer Integration anzeigen	1438
AWS-Service Integrationen	1438
Überblick über die AWS Serviceintegrationen mit Security Hub CSPM	1439
AWS Dienste, die Ergebnisse an Security Hub CSPM senden	1440
AWS Dienste, die Erkenntnisse von Security Hub CSPM erhalten	1458
Integrationen von Drittanbietern	1461
Überblick über Integrationen von Drittanbietern mit Security Hub CSPM	1461
Integrationen von Drittanbietern, die Ergebnisse an Security Hub CSPM senden	1471
Integrationen von Drittanbietern, die Ergebnisse von Security Hub CSPM erhalten	1488
Integrationen von Drittanbietern, die Ergebnisse an Security Hub CSPM senden und Ergebnisse von Security Hub empfangen	1495
Maßgeschneiderte Produktintegrationen	1497
Anforderungen und Empfehlungen für kundenspezifische Produktintegrationen	1497
Importieren von Ergebnissen aus benutzerdefinierten Produkten	1498
Beispiel für benutzerdefinierte Integrationen	1498
Ergebnisse des CSPM	1500
BatchImportFindings um Anbieter zu finden	1502
Voraussetzungen für die Verwendung von BatchImportFindings	1502
Festlegen, ob ein Ergebnis erstellt oder aktualisiert werden soll	1502
Einschränkungen beim Auffinden von Updates mit BatchImportFindings	1503
Aktualisierung der Ergebnisse mit FindingProviderFields	1503
BatchUpdateFindings für Kunden	1505
Verfügbare Felder für BatchUpdateFindings	1506
Konfiguration des Zugriffs auf BatchUpdateFindings	1506
Einzelheiten und Verlauf der Ergebnisse überprüfen	1509
Details und Verlauf der Ergebnisse überprüfen	1512
Filtern von Ergebnissen	1514
Standardfilter für Suchlisten	1515
Anweisungen zum Hinzufügen von Filtern	1515

Gruppieren der Ergebnisse	1517
Den Workflow-Status von Ergebnissen festlegen	1518
Den Workflow-Status von Ergebnissen festlegen	1520
Senden von Ergebnissen an eine benutzerdefinierte Aktion	1521
Suchformat: ASFF	1522
ASFF und Konsolidierung	1603
Erforderliche ASFF-Attribute der obersten Ebene	1665
Optionale ASFF-Attribute der obersten Ebene	1676
ResourcesASFF-Objekt	1698
Einblicke in CSPM	1822
Überprüfung und Umsetzung der Erkenntnisse	1823
Insight-Ergebnisse anzeigen und entsprechende Maßnahmen ergreifen	1823
Ergebnisse von Insight-Ergebnissen anzeigen und entsprechende Maßnahmen ergreifen (Konsole)	1825
Verwaltete Insights	1826
Benutzerdefinierte Insights	1836
Einen benutzerdefinierten Einblick erstellen	1838
Einen benutzerdefinierten Einblick bearbeiten	1841
Löschen eines benutzerdefinierten Insights	1844
CSPM-Automatisierungen	1846
Automatisierungsregeln	1847
Definition von Regelkriterien und Regelaktionen	1847
Verfügbare Regelkriterien und Regelaktionen	1848
Ergebnisse, die durch Automatisierungsregeln bewertet werden	1854
Wie funktioniert die Reihenfolge der Regeln	1855
Automatisierungsregeln erstellen	1856
Automatisierungsregeln anzeigen	1861
Automatisierungsregeln bearbeiten	1862
Reihenfolge der Regeln bearbeiten	1864
Automatisierungsregeln löschen oder deaktivieren	1865
Beispiele für Automatisierungsregeln	1867
Automatisierte Reaktion und Problembehebung	1874
EventBridge Ereignistypen	1875
EventBridge Veranstaltungsformate	1877
Eine Regel konfigurieren EventBridge	1880
Konfiguration und Verwendung benutzerdefinierter Aktionen	1887

CSPM-Dashboard	1893
Das Widget mit der Risikoübersicht	1893
Das Widget mit der Zusammenfassung der Bedrohungen	1893
Das Widget zur Sicherheitsabdeckung	1894
Verfügbare Widgets für das Übersichts-Dashboard	1894
Standardmäßig werden Widgets angezeigt	1894
Widgets sind standardmäßig ausgeblendet	1897
Das Übersichts-Dashboard filtern	1898
Filtersätze erstellen und speichern	1899
Filtersätze aktualisieren oder löschen	1900
Anpassen des Übersichts-Dashboards	1900
Regionale CSPM-Grenzwerte	1902
Regionsübergreifende Aggregationsbeschränkungen	1902
Verfügbarkeit von Integrationen nach Regionen	1902
Unterstützte Integrationen in den Regionen China (Peking) und China (Ningxia)	1902
Integrationen werden in den Regionen AWS GovCloud (USA-Ost) und (US-West) unterstützt	
AWS GovCloud	1903
Verfügbarkeit von Standards nach Regionen	1905
Verfügbarkeit von Kontrollen nach Regionen	1905
Regionale Beschränkungen der CSPM-Kontrollen	1906
USA Ost (Nord-Virginia)	1907
USA Ost (Ohio)	1908
USA West (Nordkalifornien)	1909
USA West (Oregon)	1912
Afrika (Kapstadt)	1913
Asien-Pazifik (Hongkong)	1917
Asien-Pazifik (Hyderabad)	1920
Asien-Pazifik (Jakarta)	1929
Asien-Pazifik (Malaysia)	1935
Asien-Pazifik (Melbourne)	1951
Asien-Pazifik (Mumbai)	1960
Asien-Pazifik (Osaka)	1962
Asien-Pazifik (Seoul)	1967
Asien-Pazifik (Singapur)	1970
Asien-Pazifik (Sydney)	1971
Asien-Pazifik (Taipeh)	1972

Asien-Pazifik (Thailand)	1992
Asien-Pazifik (Tokio)	2010
Kanada (Zentral)	2011
Kanada West (Calgary)	2013
China (Peking)	2029
China (Ningxia)	2038
Europa (Frankfurt)	2048
Europa (Irland)	2049
Europa (London)	2051
Europa (Milan)	2053
Europa (Paris)	2057
Europa (Spain)	2059
Europa (Stockholm)	2068
Europa (Zürich)	2070
Israel (Tel Aviv)	2078
Mexiko (Zentral)	2088
Naher Osten (Bahrain)	2107
Naher Osten (VAE)	2111
Südamerika (São Paulo)	2119
AWS GovCloud (US-Ost)	2121
AWS GovCloud (US-West)	2131
CSPM-Ressourcen erstellen mit CloudFormation	2142
Security Hub CSPM und Vorlagen AWS CloudFormation	2142
Erfahren Sie mehr über AWS CloudFormation	2143
Abonnieren von CSPM-Ankündigungen	2144
Amazon-SNS-Nachrichtenformat	2150
Security Hub CSPM deaktivieren	2152
Sicherheit	2155
Datenschutz	2156
Identity and Access Management	2157
Zielgruppe	2157
Authentifizierung mit Identitäten	2158
Verwalten des Zugriffs mit Richtlinien	2162
So funktioniert Security Hub mit IAM	2165
Beispiele für identitätsbasierte Richtlinien	2173
Service-verknüpfte Rollen	2180

AWS verwaltete Richtlinien	2184
Fehlerbehebung	2202
Compliance-Validierung	2207
Ausfallsicherheit	2208
Sicherheit der Infrastruktur	2208
VPC-Endpunkte (AWS PrivateLink)	2209
Überlegungen zu Security Hub Hub-VPC-Endpunkten	2209
Erstellen eines Schnittstellen-VPC-Endpunkts für Security Hub	2209
Erstellen einer VPC-Endpunkttrichtlinie für Security Hub	2210
Gemeinsam genutzte Subnetze	2211
Protokollieren von API-Aufrufen	2212
Security Hub CSPM-Informationen in CloudTrail	2212
Beispiel: Security Hub CSPM-Protokolldateieinträge	2213
Taggen von -Ressourcen	2215
Grundlagen des Kennzeichnens	2215
Verwenden von Tags in IAM-Richtlinien	2217
Hinzufügen von Tags	2218
Tags für Ressourcen bearbeiten	2221
Überprüfung von Stichwörtern	2223
Entfernen von Tags	2226
Kontingente	2228
Maximale Kontingente	2228
Ratenkontingente	2228
Dokumentverlauf	2229
.....	mmcccxl

Was ist AWS Security Hub?

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

AWS Security Hub ist eine einheitliche Cloud-Sicherheitslösung, die Ihre kritischen Sicherheitsprobleme priorisiert und Ihnen hilft, in großem Umfang darauf zu reagieren. Security Hub erkennt Sicherheitsprobleme, indem es Sicherheitssignale aus verschiedenen Quellen wie Posture Management, Vulnerability Management (Amazon Inspector), vertrauliche Daten (Macie) und Bedrohungserkennung () automatisch korreliert und anreichert. GuardDuty Auf diese Weise können Sicherheitsteams aktive Risiken in ihren Cloud-Umgebungen durch automatisierte Analysen und kontextuelle Einblicke priorisieren. Durch intuitive Visualisierungen wandelt Security Hub komplexe Sicherheitssignale in umsetzbare Erkenntnisse um, sodass Sie schnell fundierte Entscheidungen über Ihre Sicherheit treffen können. Security Hub umfasst auch automatisierte Reaktionsworkflows, mit denen Sie Risiken minimieren, die Teamproduktivität verbessern und Betriebsunterbrechungen minimieren können.

Features

Einheitliche Sicherheitslösung

Verschaffen Sie sich durch zentralisiertes Management in einer einheitlichen Cloud-Sicherheitslösung einen umfassenderen Überblick über Ihre gesamte Cloud-Umgebung.

Umsetzbare Einblicke in die Sicherheit

Gewinnen Sie mithilfe fortschrittlicher Analysen umsetzbare Einblicke in die Sicherheit, um mehr über die mit Ihrer Umgebung verbundenen Sicherheitsrisiken zu erfahren.

Verkürzte Reaktionszeiten

Optimieren Sie die Reaktionszeiten mit automatisierten Workflows und einem integrierten Ticketsystem.

Ergebnisse zur Exposition

Security Hub korreliert Ergebnisse von Security Hub CSPM-Kontrollprüfungen, Amazon Inspector und anderen, um Risiken im Zusammenhang AWS-Services mit Ressourcen zu erkennen. AWS

Die Ergebnisse werden im Open Cybersecurity Schema Framework (OCSF) formatiert

Security Hub generiert Ergebnisse in OCSF und erhält Ergebnisse in OCSF von Security Hub CSPM und anderen: AWS-Services

- Amazon GuardDuty
- Amazon Macie
- Amazon Inspector

Dashboard

Die Security Hub Hub-Konsole bietet einen umfassenden Überblick über Ihre Risiken, Bedrohungen, Sicherheitsabdeckung und Ressourcen sowie eine interaktive Visualisierung, das sogenannte Angriffspfaddiagramm, das zeigt, wie potenzielle Angreifer auf Ressourcen zugreifen und diese kontrollieren können, die mit einer Sicherheitslücke verknüpft sind.

Integrationen mit Produkten von Drittanbietern

Sie können Ihre Sicherheitslage mit Security Hub Hub-Integrationen verbessern. Wenn Sie beispielsweise Jira Cloud oder verwendenServiceNow ITSM, können Sie diese Funktion verwenden, um Tickets aus Ergebnissen zu erstellen.

Integrationen

Security Hub lässt sich in Folgendes integrieren AWS-Services.

- AWS Security Hub Cloud Security Posture Management (CSPM)
- Amazon GuardDuty
- Amazon Inspector
- Amazon Macie

AWS-Regionen wird für die öffentliche Vorschau unterstützt

Security Hub unterstützt Folgendes AWS-Regionen für diese öffentliche Vorschauversion.

- Asien-Pazifik (Tokio)
- Asien-Pazifik (Seoul)
- Asien-Pazifik (Osaka)
- Asia Pacific (Mumbai)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Sydney)
- Kanada (Zentral)
- Europa (Frankfurt)
- Europa (Stockholm)
- Europa (Irland)
- USA West (Nordkalifornien)
- USA West (Oregon)
- Europa (London)
- Europe (Paris)
- Südamerika (São Paulo)
- USA Ost (Nord-Virginia)
- USA Ost (Ohio)

Bei den folgenden Optionen handelt es sich um Opt-in-Optionen AWS-Regionen, bei denen Sie sie aktivieren müssen, bevor Sie darauf zugreifen können.

- Afrika (Kapstadt)
- Asien-Pazifik (Hongkong)
- Asien-Pazifik (Jakarta)
- Europa (Milan)
- Naher Osten (Bahrain)

Informationen zu diesen AWS-Regionen [Optionen finden Sie unter Opt-in-Status](#) im AWS-Regionen Availability Zones-Benutzerhandbuch.

Zugriffsmöglichkeiten

Security Hub ist in den oben AWS-Regionen aufgeführten Fällen verfügbar. Sie können Security Hub für einzelne Konten oder Konten in Ihrer Organisation aktivieren. Sie können wie folgt auf Security Hub zugreifen:

Security Hub Hub-Konsole

Die Security Hub Hub-Konsole ist eine browserbasierte Oberfläche, mit der Sie AWS Ressourcen erstellen und verwalten können. In dieser Konsole können Sie auf Ihr Konto, Ihre Daten und Ressourcen zugreifen.

Security Hub Hub-API

Die Security Hub Hub-API ermöglicht Ihnen programmatischen Zugriff auf Ihr Konto, Ihre Daten und Ressourcen. Sie können HTTPS-Anfragen direkt an Security Hub senden.

AWS CLI

Mit [dem AWS CLI](#) können Sie Befehle in der Befehlszeile Ihres Systems ausführen, um Aufgaben auszuführen, und Skripts erstellen, die Aufgaben ausführen. In einigen Fällen AWS CLI kann sie nützlicher sein als die Security Hub Hub-Konsole.

AWS SDKs

[AWS SDKs](#) besteht aus Bibliotheken und Beispielcode für verschiedene Programmiersprachen und Plattformen (C++, Go, Java, .NET und Python). Sie bieten programmatischen Zugriff auf Security Hub und andere Anwendungen AWS-Services in Ihrer bevorzugten Sprache und können Ihnen helfen, Aufgaben wie das Verwalten von Fehlern, das Signieren von Anfragen und das Wiederholen von Anfragen zu verwalten.

Preisgestaltung

Die Nutzung von Security Hub ist kostenlos. Security Hub ist während dieser öffentlichen Vorversion kostenlos.

Erste Schritte mit Security Hub

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

Die Themen in diesem Abschnitt beschreiben die ersten Schritte mit Security Hub.

Security Hub aktivieren

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

Sie können Security Hub für jeden aktivieren AWS-Konto. Die Verfahren in diesem Thema beschreiben, wie Security Hub von einem AWS Organisationsverwaltungskonto, einem delegierten Administratorkonto und einem eigenständigen Konto aus aktiviert wird.

Note

Nachdem Sie Security Hub aktiviert haben, werden die Risiken in Ihrer Umgebung sofort analysiert. Sie können jedoch bis zu 6 Stunden warten, bis Sie einen Expositionsnachweis für eine Ressource erhalten.

Security Hub für eine Organisation aktivieren

Das Verfahren in diesem Abschnitt beschreibt, wie Security Hub für das AWS Organisationsverwaltungskonto aktiviert wird. Das Verfahren geht davon aus, dass Sie einen delegierten Administrator für Security Hub CSPM eingerichtet haben, und beinhaltet einen Schritt, in dem Sie einen delegierten Administrator für Ihre Organisation in Security Hub einrichten können. Weitere Informationen zum Einrichten eines delegierten Administrators in Security Hub finden Sie unter [Ein delegiertes Administratorkonto in Security Hub einrichten](#).

Wenn Sie während der Aktivierung einen delegierten Administrator für Security Hub einrichten möchten, müssen Sie [in der AWS Organizations Konsole eine Ressourcenrichtlinie erstellen, die es](#)

[dem](#) delegierten Administrator ermöglicht, Aktionen im Namen Ihrer Organisation durchzuführen. Sie können die folgende Beispiel-Ressourcenrichtlinie für das delegierte Administratorkonto verwenden.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": [
        "organizations:AttachPolicy",
        "organizations:CreatePolicy",
        "organizations:DetachPolicy",
        "organizations>DeletePolicy",
        "organizations:UpdatePolicy",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:DisablePolicyType",
        "organizations:EnablePolicyType"
      ],
      "Resource": "*"
    }
  ]
}
```

Wenn Sie keinen delegierten Administrator einrichten, können Sie später einen delegierten Administrator einrichten. Weitere Informationen finden Sie unter [Ein delegiertes Administratorkonto in Security Hub einrichten](#). Das Thema umfasst ein Verfahren, in dem beschrieben wird, wie Sie auf der Seite Allgemein in der Security Hub Hub-Konsole einen delegierten Administrator für Ihre Organisation einrichten.

Das folgende Verfahren beschreibt, wie Sie ein delegiertes Administratorkonto für Ihre Organisation in Security Hub einrichten.

So aktivieren Sie Security Hub für ein AWS Organisationsverwaltungskonto

1. Melden Sie sich mit den Anmeldedaten Ihres AWS Organisationsverwaltungskontos bei Ihrem Konto an. AWS Öffnen Sie die Security Hub Hub-Konsole unter <https://console.aws.amazon.com/securityhub/v2/home>.
2. Wählen Sie auf der Security Hub-Startseite Security Hub aus. Wählen Sie Erste Schritte.
3. (Optional) Legen Sie für ein delegiertes Administratorkonto einen delegierten Administrator auf der Grundlage der bereitgestellten Optionen fest. Als bewährte Methode empfehlen wir, für alle Sicherheitsdienste denselben delegierten Administrator zu verwenden, um eine konsistente Verwaltung zu gewährleisten. Weitere Informationen zum Einrichten eines delegierten Administratorkontos finden Sie unter [Ein delegiertes Administratorkonto in Security Hub einrichten](#).
4. (Optional) Wählen Sie für die Kontoaktivierung das Kästchen aus, um Security Hub für Ihr AWS Konto zu aktivieren.
5. Wählen Sie Kopieren und anhängen, um die Organisationseinstellungen zu öffnen. Wählen Sie in der Organisationskonsole unter Delegierter Administrator für AWS Organizations die Option Delegieren aus und fügen Sie die Ressourcenrichtlinie ein. Wählen Sie Richtlinie erstellen aus.
6. Gehen Sie zur Security Hub Hub-Konsole. Wählen Sie Konfigurieren aus.

Wenn Sie Security Hub aktivieren, wird in Ihrem Konto eine dienstverknüpfte Rolle namens [AWSServiceRoleForSecurityHubV2](#) erstellt und Ihrem Konto wird ein dienstgebundener Rekorder hinzugefügt. Ein dienstgebundener Rekorder ist ein AWS Config Rekordertyp, der von einem AWS Dienst verwaltet wird und Konfigurationsdaten für dienstspezifische Ressourcen aufzeichnen kann. Mit einem serviceverknüpften Rekorder ermöglicht Security Hub einen ereignisgesteuerten Ansatz zum Abrufen von Ressourcenkonfigurationselementen, die für die Abdeckung der Risikoanalyse erforderlich sind. Ein serviceverknüpfter Rekorder wird pro und konfiguriert. AWS-Konto AWS-Region

Note

Wenn Sie einen delegierten Administrator einrichten, kann der delegierte Administrator eine Richtlinie erstellen und anwenden, die es ihm ermöglicht, Mitgliedskonten für Security Hub zu aktivieren und zu deaktivieren. Weitere Informationen finden Sie unter [Als delegierter Administrator eine Richtlinie zur Verwaltung von Mitgliedskonten erstellen](#).

Security Hub für den delegierten Administrator aktivieren

Wenn das AWS Organisationsverwaltungskonto einen delegierten Administrator für die Organisation festlegt, muss der delegierte Administrator Security Hub für sein Konto aktivieren. Das folgende Verfahren muss vom delegierten Administrator ausgeführt werden, jedoch nur, wenn der delegierte Administrator Security Hub nicht für sein Konto aktiviert hat. Informationen zum Einrichten eines delegierten Administrators finden Sie unter [Ein delegiertes Administratorkonto in Security Hub einrichten](#).

So aktivieren Sie Security Hub für ein delegiertes Administratorkonto

1. Melden Sie sich mit Ihren delegierten Administratoranmeldedaten bei Ihrem AWS Konto an und öffnen Sie die Security Hub Hub-Konsole unter <https://console.aws.amazon.com/securityhub/v2/home>.
2. Wählen Sie auf der Security Hub-Startseite Security Hub und dann Erste Schritte aus.
3. Wählen Sie Enable (Aktivieren) aus.
4. (Optional) Legen Sie für Tags fest, ob Sie der Kontoeinrichtung ein Schlüssel-Wert-Paar hinzufügen möchten.
5. Wählen Sie Gehe zu Security Hub.

Wenn Sie Security Hub aktivieren, wird in Ihrem Konto eine dienstverknüpfte Rolle namens [AWSServiceRoleForSecurityHubV2](#) erstellt und Ihrem Konto wird ein dienstgebundener Rekorder hinzugefügt. Ein dienstgebundener Rekorder ist ein AWS Config Rekordertyp, der von einem AWS Dienst verwaltet wird und Konfigurationsdaten für dienstspezifische Ressourcen aufzeichnen kann. Mit einem serviceverknüpften Rekorder ermöglicht Security Hub einen ereignisgesteuerten Ansatz zum Abrufen von Ressourcenkonfigurationselementen, die für die Abdeckung der Risikoanalyse erforderlich sind. Ein serviceverknüpfter Rekorder wird pro und konfiguriert. AWS-Konto AWS-Region

Note

Als delegierter Administrator für eine Organisation können Sie eine Richtlinie erstellen und anwenden, mit der Sie Mitgliedskonten für Security Hub aktivieren und deaktivieren können. Weitere Informationen finden Sie unter [Als delegierter Administrator eine Richtlinie zur Verwaltung von Mitgliedskonten erstellen](#).

Security Hub für ein eigenständiges Konto aktivieren

Das folgende Verfahren beschreibt, wie Security Hub für ein eigenständiges Konto aktiviert wird.

Es gibt zwei Arten von eigenständigen Konten, mit denen Security Hub aktiviert werden kann:

Konten außerhalb einer Organisation und Konten AWS-Konto innerhalb einer Organisation.

AWS-Konto Ein AWS-Konto unternehmensinternes System kann ein AWS System sein AWS-

Konto , an das ein delegierter Administrator eine AWS Organizations Richtlinie anhängt. AWS-

Konto Weitere Informationen finden Sie unter [Security Hub Hub-Richtlinien](#) im AWS Organizations Benutzerhandbuch.

So aktivieren Sie Security Hub für ein eigenständiges Konto

1. Melden Sie sich mit Ihren Zugangsdaten bei Ihrem AWS Konto an und öffnen Sie die Security Hub Hub-Konsole unter <https://console.aws.amazon.com/securityhub/v2/home>.
2. Wählen Sie auf der Security Hub-Startseite Security Hub und dann Erste Schritte aus.
3. Wählen Sie Enable (Aktivieren) aus.

Wenn Sie Security Hub aktivieren, wird in Ihrem Konto eine dienstverknüpfte Rolle namens

[AWSServiceRoleForSecurityHubV2](#) erstellt und Ihrem Konto wird ein dienstgebundener Rekorder

hinzugefügt. Ein dienstgebundener Rekorder ist ein AWS Config Rekordertyp, der von einem AWS

Dienst verwaltet wird und Konfigurationsdaten für dienstspezifische Ressourcen aufzeichnen kann.

Mit einem serviceverknüpften Rekorder ermöglicht Security Hub einen ereignisgesteuerten Ansatz

zum Abrufen von Ressourcenkonfigurationselementen, die für die Abdeckung der Risikoanalyse

erforderlich sind. Ein serviceverknüpfter Rekorder wird pro und konfiguriert. AWS-Konto AWS-Region

Einrichtung eines delegierten Administratorkontos in Security Hub

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

Über das AWS Organisationsverwaltungskonto können Sie einen delegierten Administrator für Ihre Organisation einrichten. Als bewährte Methode empfehlen wir, für alle Sicherheitsdienste denselben delegierten Administrator zu verwenden, um eine konsistente Verwaltung zu gewährleisten. In den Verfahren in diesem Abschnitt wird beschrieben, wie Sie auf zwei Arten einen delegierten Administrator für Ihr Unternehmen einrichten können. Die erste Möglichkeit besteht in einem AWS Organisationsverwaltungskonto, für das kein delegierter Administrator in Security Hub CSPM

festgelegt wurde. Die zweite Möglichkeit besteht für ein AWS Organisationsverwaltungs-konto, das Security Hub aktiviert, aber bei der Aktivierung die Einstellung eines delegierten Administrators übersprungen hat.

Überlegungen

Möglicherweise stoßen Sie auf ein Szenario, in dem Sie einen delegierten Administrator für Security Hub einrichten möchten, der sich vom delegierten Administrator für Security Hub CSPM unterscheidet. Wenn Sie in Security Hub CSPM einen delegierten Administrator eingerichtet haben, sollten Sie Folgendes beachten:

- Wenn das AWS Organisationsverwaltungs-konto als delegierter Administrator für Security Hub CSPM eingerichtet ist, können Sie dieses Konto nicht als delegierten Administrator für Security Hub einrichten. Sie können jedoch einen anderen Mitarbeiter AWS-Konto der Organisation als delegierten Administrator für Security Hub benennen. Für eine konsistente Verwaltung aller Sicherheitsdienste empfehlen wir, dasselbe Konto (mit Ausnahme des AWS Organisationsverwaltungs-kontos) wie der delegierte Administrator für Security Hub CSPM und Security Hub zu verwenden.
- Wenn ein anderes Konto als das AWS Organisationsverwaltungs-konto als delegierter Administrator für Security Hub CSPM eingerichtet ist, wird dieses Konto automatisch zum delegierten Administrator in Security Hub. In diesem Szenario erlaubt Security Hub nur diesem Benutzer, als delegierter Administrator AWS-Konto zu fungieren.

Note

Wenn Sie als delegierter Security Hub CSPM-Administrator ein anderes Konto als das Organisationsverwaltungs-konto verwenden, wird es durch das Entfernen entweder über die Security Hub CSPM-Konsole oder die Organisations API auch AWS aus Security Hub entfernt. Wenn Sie den delegierten Security Hub-Administrator über die Security Hub-Konsole oder die AWS Organisations-API entfernen, wird er auch aus Security Hub CSPM entfernt. Wenn der delegierte Administrator aus Security Hub CSPM entfernt wird, deaktiviert sich die Zentralkonfiguration automatisch.

Beim folgenden Verfahren wird davon ausgegangen, dass Sie keinen delegierten Administrator für Security Hub CSPM eingerichtet haben und einen delegierten Administrator für Security Hub einrichten.

So richten Sie einen delegierten Administrator in Security Hub ein

1. Melden Sie sich mit den Anmeldeinformationen Ihres AWS Organisationsverwaltungskontos bei Ihrem Konto an und öffnen Sie die Security Hub Hub-Konsole unter <https://console.aws.amazon.com/securityhub/v2/home>.
2. Wählen Sie auf der Security Hub-Startseite Security Hub und dann Erste Schritte aus.
3. Wählen Sie unter Delegierter Administrator die Option Konfigurieren aus. Geben Sie im Popup-Fenster die 12-stellige AWS-Konto Zahl für AWS-Konto das gewünschte Konto ein, oder wählen Sie ein empfohlenes Konto aus (falls Sie delegierte Administratoren in anderen Sicherheitsdiensten verwenden), das Sie als delegierten Administrator für Ihr Unternehmen festlegen möchten. Wählen Sie Speichern.
4. (Optional) Wählen Sie für die Kontoaktivierung das Kästchen aus, um Security Hub für Ihr zu aktivieren. AWS-Konto
5. Wählen Sie Kopieren und Anhängen, um die Organisationseinstellungen zu öffnen. Wählen Sie in der Organisationskonsole unter Delegierter Administrator für AWS Organizations die Option Delegieren aus und fügen Sie die Ressourcenrichtlinie ein. Wählen Sie Richtlinie erstellen aus.
6. Gehen Sie zur Security Hub Hub-Konsole. Wählen Sie Konfigurieren aus.

Note

Nachdem Sie den delegierten Administrator eingerichtet haben, muss dieses Konto [Security Hub aktivieren](#) und Richtlinien konfigurieren, um Ergebnisse von seinem Mitgliedskonto zu erhalten.

Das folgende Verfahren geht davon aus, dass Sie Security Hub aktiviert, aber bei der Aktivierung die Einstellung eines delegierten Administrators übersprungen haben. Auf der Seite Allgemein können Sie in der Security Hub Hub-Konsole einen delegierten Administrator einrichten.

So richten Sie in der Security Hub Hub-Konsole auf der Seite Allgemein einen delegierten Administrator ein

1. Melden Sie sich mit den Anmeldeinformationen Ihres AWS Organisationsverwaltungskontos bei Ihrem Konto an und öffnen Sie die Security Hub Hub-Konsole unter <https://console.aws.amazon.com/securityhub/v2/home>.
2. Wählen Sie im Navigationsbereich die Option Allgemein aus.

3. Wählen Sie unter Delegierter Administrator die Option Konfigurieren aus. Geben Sie im Pop-up-Fenster die 12-stellige AWS-Konto Zahl für die Person ein AWS-Konto, die Sie als delegierten Administrator für Ihre Organisation festlegen möchten. Oder wählen Sie einen Vorschlag, AWS-Konto wenn Sie in anderen AWS Sicherheitsdiensten einen delegierten Administrator einrichten möchten. Wählen Sie Speichern.

Nachdem Sie dieses Verfahren abgeschlossen haben, müssen Sie die Erklärung zur Delegierungsrichtlinie für Security Hub kopieren und sie Ihrem delegierten Administrator für AWS Organizations Richtlinien beifügen, damit der delegierte Administrator für Security Hub Aktionen in Security Hub ausführen kann. Ohne diese Richtlinienerklärung kann der delegierte Administrator Security Hub nicht für Ihr Unternehmen konfigurieren. Weitere Informationen finden Sie unter [Die Erklärung zur Delegierungsrichtlinie für Security Hub anhängen](#).

Die Erklärung zur Delegierungsrichtlinie für Security Hub anhängen

Aus dem Organisationsverwaltungs-konto müssen Sie die Erklärung zur Delegierungsrichtlinie für Security Hub kopieren und sie an Ihren delegierten Administrator für AWS Organizations Richtlinien anhängen, damit der delegierte Administrator für Security Hub Aktionen in Security Hub ausführen kann. Ohne diese Richtlinienerklärung kann der delegierte Administrator Security Hub nicht für Ihr Unternehmen konfigurieren. Sie können diese Richtlinie von der Seite Allgemein in der Security Hub Hub-Konsole kopieren. Wenn Sie dies tun, werden Sie auf die Seite „Einstellungen“ in der AWS Organizations Konsole weitergeleitet, auf der Sie die AWS Organizations Richtlinie für Ihren delegierten Administrator bearbeiten können. In diesem Thema wird beschrieben, wie Sie die Richtlinie in Security Hub kopieren. Informationen zum Aktualisieren der AWS Organizations Richtlinie für den delegierten Administrator finden Sie unter [Aktualisieren einer ressourcenbasierten Delegierungsrichtlinie mit AWS Organizations](#) im AWS Organizations Benutzerhandbuch.

So fügen Sie die Erklärung zur Delegierungsrichtlinie für Security Hub bei

1. Melden Sie sich mit den Anmeldeinformationen Ihres AWS Organisationsverwaltungs-kontos bei Ihrem Konto an und öffnen Sie die Security Hub Hub-Konsole unter <https://console.aws.amazon.com/securityhub/v2/home>.
2. Wählen Sie im Navigationsbereich die Option Allgemein aus.
3. Wählen Sie in der Richtlinienerklärung zur Delegierung für Security Hub die Option Kopieren und anhängen aus. Sie werden auf die Seite Einstellungen weitergeleitet, auf der Sie die AWS Organizations Richtlinie Ihres delegierten Administrators so bearbeiten können, dass die

Erklärung zur Delegierungsrichtlinie hinzugefügt wird. AWS Organizations Wenn Sie sich die Richtlinienerklärung ansehen möchten, bevor Sie sie kopieren, wählen Sie Richtlinienetails.

 Note

Wenn Sie einen delegierten Administrator einrichten, kann der delegierte Administrator eine Richtlinie erstellen und anwenden, die es ihm ermöglicht, Mitgliedskonten zu aktivieren und zu deaktivieren. Das Verfahren im folgenden Thema beschreibt, wie Sie diese Richtlinie einrichten.

Als delegierter Administrator eine Richtlinie zur Verwaltung von Mitgliedskonten erstellen

Als delegierter Administrator für eine Organisation können Sie eine Richtlinie erstellen und anwenden, mit der Sie Mitgliedskonten aktivieren und deaktivieren können. Sie können über den Konfigurationsbildschirm der Security Hub Hub-Konsole auf alle Ihre konfigurierten Richtlinien zugreifen. Das folgende Verfahren beschreibt, wie Sie diese Richtlinie erstellen.

 Note

Schritt 6 ist ein optionaler Schritt, in dem Sie beschreiben können, wie diese Richtlinie mit übergeordneten Richtlinien interagiert. Informationen zur Vererbung von Richtlinien finden Sie unter [Grundlegendes zur Vererbung von Verwaltungsrichtlinien](#) im AWS Organizations Benutzerhandbuch.

Um eine Richtlinie zu erstellen, mit der Sie Mitgliedskonten aktivieren und deaktivieren können

1. Melden Sie sich mit Ihren Anmeldeinformationen an und öffnen Sie die Security Hub Hub-Konsole unter <https://console.aws.amazon.com/securityhub/v2/home? region=us-ost-1>.
2. Wählen Sie im Navigationsbereich Einstellungen und dann Konfigurationen aus.
3. Wählen Sie Richtlinie erstellen aus.
4. Geben Sie unter Details einen Namen für die Richtlinie ein und legen Sie fest, ob Sie eine optionale Beschreibung für die Richtlinie eingeben möchten.
5. Wählen Sie für Regionen die Option Alle Regionen aktivieren, Alle Regionen deaktivieren oder Regionen angeben aus. Wenn Sie „Alle Regionen aktivieren“ wählen, können Sie festlegen,

ob neue Regionen automatisch aktiviert werden sollen. Wenn Sie Alle Regionen deaktivieren wählen, können Sie festlegen, ob neue Regionen automatisch deaktiviert werden sollen. Wenn Sie „Regionen angeben“ wählen, müssen Sie auswählen, welche Regionen Sie aktivieren und deaktivieren möchten.

6. (Optional) Informationen zu den erweiterten Einstellungen finden Sie in der [Anleitung](#) von AWS Organizations.
7. (Optional) Legen Sie für Tags fest, ob der Richtlinie ein Schlüssel-Wert-Paar hinzugefügt werden soll. Sie können bis zu 50 Tags hinzufügen.
8. Wählen Sie Weiter aus.
9. Überprüfen Sie Ihre Änderungen und wählen Sie dann Anwenden aus. Ihre Zielkonten werden auf der Grundlage der Richtlinie konfiguriert. Um zu sehen, welche Richtlinie auf Kontoebene gültig ist, können Sie auf der Konfigurationsseite die Registerkarte Organisation aufrufen, auf der Sie ein Konto auswählen können.

Das delegierte Administratorkonto in Security Hub entfernen

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

Sie können das delegierte Administratorkonto jederzeit in der Security Hub Hub-Konsole entfernen. Diese Aktion entfernt jedoch nicht nur den delegierten Administrator aus Security Hub, sondern auch Security Hub CSPM. Wir empfehlen, diese Aktion nur durchzuführen, wenn Sie diesen Vorgang mit Ihrem Sicherheitskonto bestätigt haben.

Note

Wenn Sie als delegierter Security Hub-CSPM-Administrator ein anderes Konto als das Organisationsverwaltungskonto verwenden, wird es durch das Entfernen entweder über die CSPM-Konsole oder die AWS Organizations API auch aus Security Hub entfernt. Wenn Sie den delegierten Security Hub-Administrator entweder über die Security Hub-Konsole oder die AWS Organizations API entfernen, wird er auch aus Security Hub CSPM entfernt. Wenn der delegierte Administrator aus CSPM entfernt wird, wird die zentrale Konfiguration automatisch deaktiviert.

Um das delegierte Administratorkonto zu entfernen

1. Melden Sie sich mit den Anmeldeinformationen Ihres AWS Organisationsverwaltungskontos bei Ihrem Konto an und öffnen Sie die Security Hub Hub-Konsole unter <https://console.aws.amazon.com/securityhub/v2/home?region=us-ost-1>.
2. Wählen Sie im Navigationsbereich die Option Allgemein aus.
3. Wählen Sie unter Delegierter Administrator die Option Delegierten Administrator entfernen aus. Geben Sie im Popup-Fenster Bestätigen ein und wählen Sie Entfernen aus.

Security Hub Hub-Empfehlungen

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

Die folgenden Sicherheitsdienste AWS senden Ergebnisse im OCSF-Format an Security Hub. Nachdem Sie Security Hub aktiviert haben, empfehlen wir, diese AWS-Services für zusätzliche Sicherheit zu aktivieren.

Security Hub CSPM

Wenn Sie [Security Hub CSPM aktivieren](#), erhalten Sie einen umfassenden Überblick über Ihren Sicherheitsstatus in AWS. Auf diese Weise können Sie Ihre Umgebung anhand von Industriestandards und bewährten Methoden beurteilen. Sie können zwar mit Security Hub beginnen, ohne Security Hub CSPM zu aktivieren, wir empfehlen jedoch, Security Hub CSPM zu aktivieren, da Security Hub Sicherheitssignale von Security Hub CSPM korreliert, um Ihr Statusmanagement zu verbessern.

Wenn Sie [Security Hub CSPM aktivieren](#), empfehlen wir außerdem, [den Standard AWS Foundational Security Best Practices für Ihr Konto zu aktivieren](#). Dieser Standard besteht aus einer Reihe von Kontrollen, die erkennen, wenn Sie AWS-Konten und Ihre Ressourcen von den bewährten Sicherheitsmethoden abweichen. Wenn Sie den Standard AWS Foundational Security Best Practices für Ihr Konto aktivieren, aktiviert AWS Security Hub Cloud Security Posture Management (CSPM) automatisch alle seine Kontrollen, einschließlich der Kontrollen für die folgenden Ressourcentypen:

- Kontosteuerungen
- DynamoDB-Steuerelemente

- EC2 Amazon-Kontrollen
- IAM-Steuerelemente
- AWS Lambda steuert
- Amazon RDS-Steuerelemente
- Amazon S3 S3-Steuerelemente

Sie können alle Steuerelemente in dieser Liste deaktivieren. Wenn Sie jedoch eines dieser Steuerelemente deaktivieren, können Sie keine Expositionsergebnisse für unterstützte Ressourcen erhalten. Informationen zu Kontrollen, die für den Standard AWS Foundational Security Best Practices gelten, finden Sie unter [AWS Foundational Security Best Practices v1.0.0 \(FSBP\)](#).

GuardDuty

Wenn Sie die GuardDuty Option [aktivieren](#), können Sie alle Ihre Ergebnisse zu Bedrohungen und Sicherheitsvorkehrungen im Dashboard der Security Hub Hub-Konsole einsehen. Wenn Sie diese Option aktivieren GuardDuty, GuardDuty wird automatisch mit dem Senden von Daten an Security Hub im OCSF-Format begonnen.

Amazon Inspector

Wenn Sie [Amazon Inspector aktivieren](#), können Sie alle Ihre Risiken und Ergebnisse zur Sicherheitsabdeckung im Dashboard der Security Hub Hub-Konsole einsehen. Wenn Sie Amazon Inspector aktivieren, beginnt Amazon Inspector automatisch, Daten im OCSF-Format an Security Hub zu senden.

Wir empfehlen, das EC2 Amazon-Scannen und das Lambda-Standardscannen zu aktivieren. Wenn Sie EC2 Amazon-Scanning aktivieren, scannt Amazon Inspector EC2 Amazon-Instances in Ihrem Konto auf Paketschwachstellen und Probleme mit der Netzwerkerreichbarkeit. Wenn Sie das Lambda-Standardscannen aktivieren, scannt Amazon Inspector Lambda-Funktionen auf Softwareschwachstellen in Paketabhängigkeiten. Weitere Informationen finden Sie unter [Aktivierung eines Scan-Typs](#) im Amazon Inspector Inspector-Benutzerhandbuch.

Macie

Wenn Sie [Macie aktivieren](#), können Sie zusätzliche Risiken für Ihre Amazon S3 S3-Buckets erkennen. Wir empfehlen, die [automatische Erkennung sensibler Daten](#) zu konfigurieren, damit Macie Ihr Amazon S3 S3-Bucket-Inventar täglich auswerten kann.

Security Hub Hub-Konzepte

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

Die folgenden Begriffe und Konzepte sollen Ihnen helfen zu verstehen, wie Sie mit Expositionsergebnissen umgehen können.

Exposition

Ein potenzielles Sicherheitsszenario in Ihrem Konto, das auf Sicherheitslücken, ausnutzbare Ressourcen oder Fehlkonfigurationen zurückzuführen sein kann.

Feststellung der Gefährdung

Eine Art von Befund, der eine in Ihrer Umgebung vorhandene Exposition beschreibt. Ein Expositionsergebnis umfasst Merkmale und Signale. Ein Signal kann eine oder mehrere Arten von Expositionsmerkmalen enthalten. Security Hub generiert eine Risikofeststellung, wenn Signale von Security Hub CSPM-Kontrollergebnissen oder anderen Quellen AWS-Services, wie Amazon Inspector, auf das Vorliegen einer Gefährdung hinweisen. Für eine Ressource kann höchstens ein Expositionsergebnis vorliegen. Security Hub generiert eine Risikofeststellung, wenn eine Ressource gefährdet ist. Wenn eine Ressource keine oder nur unzureichende Merkmale aufweist, generiert Security Hub für diese Ressource keine Gefährdungsermittlung.

Signal

Ein Befund, der zu einer Expositionsfeststellung beiträgt. Ein Signal kann als beitragendes Ergebnis bezeichnet werden. Ein Signal kann von Security Hub, CSPM oder einem anderen AWS Config System wie Amazon AWS-Services Inspector stammen.

Merkmal

Eine Sicherheitsabweichung, die zu einer Risikofeststellung führt. Zu den Merkmalstypen gehören Fehlkonfiguration, Erreichbarkeit, sensible Daten und Sicherheitslücke. Ein Merkmal ist mit einem Signal verknüpft, und ein Signal kann mehrere Merkmale enthalten. Ein Security Hub CSPM-Steuerelement weist beispielsweise darauf hin, dass eine vom Kunden verwaltete Richtlinie eine administrative Zugriffskontrolle ermöglicht. Dieses Signal enthält ein Merkmal einer Fehlkonfiguration.

OCSF-Ergebnisse im Security Hub

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

Alle Ergebnisse in Security Hub sind im Open Cybersecurity Schema Framework (OCSF) formatiert. Security Hub betrachtet Ergebnisse mit `activity_name != Close` als aktive Ergebnisse. Aktive Ergebnisse werden automatisch gelöscht, wenn sie innerhalb von 90 Tagen nicht aktualisiert werden. Security Hub betrachtet Ergebnisse mit `Activity_name = Close` als abgeschlossene Ergebnisse. Geschlossene Ergebnisse werden automatisch gelöscht, wenn sie innerhalb von 14 Tagen nicht aktualisiert werden. Security Hub bestimmt anhand des neuesten Werts des Ergebnisses, wann ein Ergebnis aktualisiert wird `modified_time_dt`. Am Ende der Aufbewahrungsfrist eines Befundes löscht Security Hub den Befund dauerhaft. Die Suche nach Anbietern kann den Wert des `finding.info.modified_time_dt` Felds ändern, wenn sie einen Befund aktualisieren. Informationen zu anderen `Activity_name` Werten finden Sie unter [Suche nach Sicherheitslücken](#) im OCSF-Schema.

Deckungsergebnisse im Security Hub

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

Die Ergebnisse der Sicherheitsabdeckung für Security Hub geben Aufschluss AWS darüber, welche Sicherheitsfunktionen aktiviert sind und wo es in einem eigenständigen Konto oder in der gesamten AWS Unternehmensumgebung möglicherweise Lücken in der Abdeckung gibt. Durch die Aktivierung zusätzlicher Sicherheitsfunktionen werden die Erkennungsfunktionen von Security Hub verbessert. In den Ergebnissen der Berichterstattung wird bewertet GuardDuty, welche CSPM-Funktionen von Amazon Inspector, Macie und Security Hub für ein Konto aktiviert sind. Diese Ergebnisse werden als Widget auf dem Security Hub-Dashboard angezeigt und bieten die Möglichkeit, detailliertere Ansichten nach bestimmten Sicherheitsfunktionen aufzurufen. Für den delegierten Administrator zeigt dieses Widget die Aufschlüsselung der Abdeckung für alle Security Hub Hub-aktivierten Konten.

Einschränkungen

- Bei Mitgliedskonten werden die Deckungsinformationen für alle verknüpften Konten zusammengefasst AWS-Regionen, jedoch nur für dieses Mitgliedskonto.
- Für Konten, die nicht in Security Hub integriert sind, werden keine Deckungsinformationen angezeigt
- Der Versicherungsschutz gibt nur an, ob ein aktiviert AWS-Service ist, nicht, ob bestimmte Funktionen in einem AWS Dienst aktiviert sind.

Deckungsergebnisse für Security Hub CSPM

In den Ergebnissen der CSPM-Abdeckung von Security Hub wird bewertet, ob in einem Konto ein qualifizierter Sicherheitsstandard zur Posture Management aktiviert ist. Die Aktivierung eines beliebigen Security Hub CSPM-Standards ist zulässig, mit Ausnahme der Standards AWS Control Tower und der Resource Tagging-Standards.

Es kann bis zu 24 Stunden dauern, bis die standardmäßig aktivierten Standards erkannt werden, wenn Security Hub CSPM aktiviert wird.

Ergebnisse der Berichterstattung für GuardDuty

GuardDuty Anhand der Ergebnisse zur Abdeckung GuardDuty wird bewertet, ob und welche GuardDuty Funktionen aktiviert sind in einem AWS-Konto:

- Malware-Schutz für Amazon EC2 — Scannt EC2 Amazon-Instances nach potenzieller Malware
- Amazon EKS Protection — Überwacht Kubernetes-Auditprotokolle auf Bedrohungen in Amazon EKS-Clustern
- Lambda-Schutz — Analysiert Lambda-Funktionsaufrufe im Hinblick auf potenzielle Bedrohungen
- Amazon S3 S3-Schutz — Analysiert Datenereignisse im Hinblick auf potenzielle Bedrohungen für Amazon S3 S3-Buckets
- Amazon RDS Protection — Überwacht Amazon RDS-Datenbanken auf Bedrohungen
- Laufzeitüberwachung — Ermöglicht die Echtzeitüberwachung des Laufzeitverhaltens in EC2 Amazon-Instances

Es kann bis zu 24 Stunden dauern, bis Aktualisierungen des GuardDuty Versicherungsschutzes für alle Mitgliedskonten einer Organisation übernommen werden.

Ergebnisse der Berichterstattung für Amazon Inspector

In den Ergebnissen der Berichterstattung von Amazon Inspector wird geprüft, ob Amazon Inspector aktiviert ist und welche Funktionen in einem Konto aktiviert sind:

- Amazon EC2 Scanning — Scannt EC2 Amazon-Instances auf Sicherheitslücken
- Amazon ECR Scanning — Scannt Container-Images in Amazon ECR auf Sicherheitslücken
- Lambda Standard Scanning — Scannt Lambda-Funktionen auf Sicherheitslücken
- Lambda-Code-Scanning — Scannt Lambda-Code-Funktionen auf Code-Schwachstellen
- Amazon Inspector Code Security — Scannt den Quellcode von Erstanbieteranwendungen, Abhängigkeiten von Drittanbieteranwendungen und Infrastructure as Code auf Sicherheitslücken

Ergebnisse der Berichterstattung für Macie

Bei den Ergebnissen der Macie-Abdeckung handelt es sich um Bewertungen, aus denen hervorgeht, ob Macie Across aktiviert ist. AWS-Konten

Es kann bis zu 24 Stunden dauern, bis Aktualisierungen der automatisierten Erkennung sensibler Daten von Macie für alle Mitgliedskonten einer Organisation übernommen werden.

Ergebnisse der Sicherheitslücke im Security Hub

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

Security Hub korreliert Ergebnisse von Security Hub CSPM-Kontrollprüfungen und anderen AWS-Services, z. B. Amazon Inspector, um Risiken im Zusammenhang mit Ressourcen zu erkennen. AWS Ein Sicherheitsrisiko ist eine Art von Feststellung, die eine potenzielle Gefährdung in Ihrer Umgebung aufgrund von Sicherheitslücken, ausnutzbaren Ressourcen oder Fehlkonfigurationen beschreibt. Indem Sie Ihre kritischsten Sicherheitsrisiken priorisieren und beheben, können Sie potenzielle Angriffe auf Ihre Umgebung verhindern. Sie können in der Security Hub-Konsole und programmgesteuert mit Security Hub CSPM- und Security Hub-API-Vorgängen auf Ihre Ergebnisse zur Gefährdung zugreifen.

Unterstützte Ressourcentypen für Risikoperggebnisse in Security Hub

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

Security Hub generiert Risikoperggebnisse für die folgenden AWS Ressourcentypen:

- `AWS::DynamoDB::Table`
- `AWS::EC2::Instance`
- `AWS::ECS::Service`
- `AWS::EKS::Cluster`
- `AWS::IAM::User`
- `AWS::Lambda::Function`
- `AWS::RDS::DBInstance`
- `AWS::S3::Bucket`

Security Hub generiert einen Risikobefund pro Ressource. Wenn eine Ressource keine oder nur unzureichende Merkmale aufweist, generiert Security Hub für diese Ressource keine Gefährdungsermittlung.

Unterstützte Merkmalstypen in Security Hub

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

Security Hub generiert einen Risikobefund, wenn AWS Security Hub Cloud Security Posture Management (CSPM) -Kontrollergebnisse und Ergebnisse AWS-Services, die von anderen unterstützten Programmen wie Amazon Inspector generiert wurden, Risikomerkmale für eine Ressource enthalten. Die folgende Tabelle enthält Informationen zu den unterstützten Merkmalstypen.

Merkmalstyp	Beschreibung	Quelle	Betroffene Ressourcen
Fehlkonfiguration	Weist auf eine falsch konfigurierte Ressource hin.	Ergebnisse der Security Hub CSPM-Kontrolle.	Alle Ressourcentypen.
Erreichbarkeit	Weist auf offene Netzwerkpfade zu einer Ressource hin.	Ergebnisse der Security Hub CSPM-Kontrolle und Ergebnisse der Amazon Inspector Inspector-Netzwerk erreichbarkeit.	EC2 Amazon-Instanzen
Sensible Daten	Zeigt an, dass eine Ressource sensible Daten enthält.	Macie-Ergebnisse mit sensiblen Daten.	Amazon-S3-Buckets
Sicherheitslücke	Weist darauf hin, dass eine Ressource häufigen Sicherheitslücken und Gefahren ausgesetzt ist (CVEs).	Ergebnisse der Sicherheitslücke im Amazon Inspector-Paket.	EC2 Amazon-Instanzen, Amazon ECS-Services, Amazon EKS-Cluster und Lambda-Funktionen

Jedes Merkmal kann mit mehreren Titeln verknüpft werden, die Einzelheiten über die Exposition enthalten, die sich auf die Ressource auswirkt. Beispielsweise könnten Sie in den Details für ein gefundenes EC2 Risiko den Titel Exploit Available für das Merkmal Sicherheitslücke sehen.

Generierung von Ergebnissen zur Gefährdung

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

Security Hub generiert alle 6 Stunden Ergebnisse zur Gefährdung. In jedem Zeitraum von 6 Stunden berücksichtigt Security Hub die verfügbaren Expositionsmerkmale für eine Ressource. Pro Ressourcen-ID wird maximal ein Expositionsbefund generiert. Die Eindeutigkeit eines Ergebnisses hängt von der ID AWS-Region, dem Typ und dem Konto ab. Das bedeutet, dass Sie zwei Ressourcen mit derselben ID haben können, es sich jedoch um unterschiedliche Ressourcentypen handeln würde. Dieser Expositionsergebnis fasst alle zutreffenden Expositionsmerkmale zusammen, die für die Ressource gelten.

Wenn eine Ressource keine oder nur unzureichende Merkmale aufweist, generiert Security Hub für diese Ressource keine Gefährdungsermittlung. Security Hub veröffentlicht keine Risikopergebnisse für Ressourcentypen, die keine Risikoergebnisse unterstützen. Wenn eine Ressource eine signifikante Anzahl und Kombination von Merkmalen aufweist, generiert Security Hub einen Risikobefund. Die Anzahl und Kombination der Merkmale bestimmen auch den Schweregrad des Expositionsergebnisses.

Expositionsergebnis der Stichprobe

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

Security Hub normalisiert die Ergebnisse der Sicherheitslücken im Open Cybersecurity Schema Framework (OCSF).

Beispiel für ein OCSF-Schema

Im folgenden Beispiel für ein OCSF-Schema enthält der `related_events` Parameter Details, die sich nur auf das Expositionsergebnis beziehen, wie z. B. beitragende Ergebnisse. Zu den Ergebnissen beitragen die Merkmale und Signale, die mit einem Expositionsergebnis in Verbindung stehen. Ein einzelnes beitragendes Ergebnis kann ein oder mehrere Merkmale umfassen. Der

observables Parameter identifiziert die Ressource, die dem beitragenden Ergebnis zugeordnet ist. Dies kann sich von dem resources Parameter unterscheiden, der die Ressource identifiziert, die mit dem Expositionsergebnis verknüpft ist.

```
{
  "activity_id": 1,
  "activity_name": "Create",
  "category_name": "Findings",
  "category_uid": 2,
  "class_name": "Detection Finding",
  "class_uid": 2004,
  "cloud": {
    "account": {
      "uid": "123456789012",
      "name": "production-application"
    },
    "cloud_partition": "aws",
    "provider": "AWS",
    "region": "us-east-1"
  },
  "finding_info": {
    "analytic": {
      "name": "Exposure",
      "type": "Rule",
      "type_id": 1,
      "uid": "0.0.1"
    },
    "created_time_dt": "2024-11-15T21:39:26.337224100Z",
    "desc": "Publicly invocable Lambda function executed outside of VPC has vulnerability with known exploit that can be exploited from remote network",
    "finding_info.modified_time_dt": "2024-11-15T21:39:26.337224100Z",
    "related_events_count": 3,
    "related_events": [
      {
        "tags": [
          {
            "name": "Vulnerability",
            "values": [
              "Attack Vector Network",
              "EPSS Level >= High",
              "EPSS Level >= Medium",
              "Exploit Available",
              "No Privileges Required",
            ]
          }
        ]
      }
    ]
  }
}
```

```

        "No User Interaction Required",
        "Vulnerable"
    ]
}
],
"product": {
    "uid": "arn:aws:securityhub:us-east-1::productv2/aws/inspector"
},
"observables": [
    {
        "type": "Resource UID",
        "type_id": 10,
        "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"
    }
],
"type": "Finding",
"title": "CVE-2023-33246 - org.apache.rocketmq:rocketmq-controller",
"uid": "arn:aws:inspector2:us-
east-1:123456789012:finding/1234567890abcdef0"
},
{
    "tags": [
        {
            "name": "Reachability",
            "values": [
                "Publicly Invocable"
            ]
        }
    ],
    "product": {
        "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub"
    },
    "observables": [
        {
            "type": "Resource UID",
            "type_id": 10,
            "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"
        }
    ],
    "type": "Finding",
    "title": "Lambda function policies should prohibit public access",

```

```

      "uid": "arn:aws:securityhub:us-east-1:123456789012:security-control/
Lambda.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
    },
    {
      "tags": [
        {
          "name": "Misconfiguration",
          "values": [
            "Deployed outside VPC"
          ]
        }
      ],
      "product": {
        "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub"
      },
      "observables": [
        {
          "type": "Resource UID",
          "type_id": 10,
          "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"
        }
      ],
      "type": "Finding",
      "title": "Lambda functions should be in a VPC",
      "uid": "arn:aws:securityhub:us-east-1:123456789012:security-control/
Lambda.3/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
    }
  ],
  "title": "Publicly invocable Lambda function executed outside of VPC has
vulnerability with known exploit that can be exploited from remote network",
  "types": [
    "Exposure/Potential Impact/Resource Hijacking"
  ],
  "uid": "arn:aws:securityhub:us-
east-1:123456789012:risk:1234f781c7ae7507f01e2fb460f15ca8fe7f9c95e257698a092cb74a4ea84a42"
},
"metadata": {
  "product": {
    "name": "Security Hub Exposure Analysis",
    "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub-risk",
    "vendor_name": "Amazon"
  },
  "processed_time_dt": "2024-11-15T21:39:58.819Z",

```

```

    "profiles": [
      "cloud",
      "datetime"
    ],
    "version": "1.4.0-dev"
  },
  "resources": [
    {
      "cloud_partition": "aws",
      "region": "us-east-1",
      "tags": [
        {
          "name": "aws:cloudformation:stack-name",
          "value": "VeepLambdaRule3"
        },
        {
          "name": "aws:cloudformation:stack-id",
          "value": "arn:aws:cloudformation:us-east-1:123456789012:stack/
VeepLambdaRule3/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222"
        },
        {
          "name": "aws:cloudformation:logical-id",
          "value": "lambdar3function94D10D40"
        }
      ],
      "type": "AwsLambdaFunction",
      "uid": "arn:aws:lambda:us-east-1:123456789012:application-function"
    }
  ],
  "severity": "Critical",
  "severity_id": 5,
  "status": "New",
  "status_id": 1,
  "time": 1731706766337,
  "time_dt": "2024-11-15T21:39:26.337224100Z",
  "type_name": "Detection Finding: Create",
  "type_uid": 200401,
  "vendor_attributes": {
    "severity_id": 5,
    "severity": "Critical"
  }
}

```

Bestimmung des Schweregrads eines Expositionsergebnisses

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

Security Hub weist jedem Sicherheitsrisiko, das entdeckt wird, einen Standardschweregrad von CRITICAL, HIGHMEDIUM, oder LOW zu. Expositionsergebnisse mit einem Schweregrad von INFORMATIONAL werden nicht veröffentlicht. Security Hub verwendet mehrere Faktoren, um den Standardschweregrad einer Risikofeststellung zu bestimmen:

- **Sensibilisierung** — Das Ausmaß, in dem die Gefahr nicht theoretisch ist, sondern öffentlich zugängliche oder automatisierte Exploits beinhaltet. Dies gilt für Expositionsergebnisse für EC2 Instances und Lambda-Funktionen.
- **Einfache Erkennung** — Ob automatisierte Tools wie ein Port-Scan oder eine Internetsuche zur Verfügung stehen, um die gefährdete Ressource zu entdecken.
- **Einfache Ausnutzung** — Die Leichtigkeit, mit der ein Bedrohungsakteur die Gefahr ausnutzen kann. Wenn beispielsweise offene Netzwerkpfade oder falsch konfigurierte Metadaten existieren, kann ein Bedrohungsakteur die Gefahr leichter ausnutzen.
- **Wahrscheinlichkeit eines Exploits** — Die Wahrscheinlichkeit, dass das Sicherheitsrisiko in den nächsten 30 Tagen ausgenutzt wird. Dieser Faktor entspricht dem Exploit Protection Scoring System (EPSS) und gilt für Risikoperegebnisse für EC2 Amazon-Instances und Lambda-Funktionen.
- **Auswirkung** — Der Schaden, der entsteht, wenn der Exploit ausgeführt wird. Eine Offenlegung könnte beispielsweise zum Verlust der Rechenschaftspflicht, zum Verlust der Verfügbarkeit, zum Verlust der Vertraulichkeit aufgrund der Offenlegung von Daten oder zum Verlust der Integrität aufgrund von Datenbeschädigung führen.

Überprüfung der Ergebnisse zur Exposition

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

Sie können alle Ihre Erkenntnisse zur Gefährdung in der AWS Security Hub Hub-Konsole und mit der API überprüfen. Auf der Seite Exposures in der Security Hub Hub-Konsole werden alle aktiven Risikoergebnisse angezeigt. Die Ergebnisse der Exposition werden nach abnehmendem Schweregrad aufgelistet. Sie können Ihre Expositionsergebnisse filtern, indem Sie Filter mit der Suchleiste Filter hinzufügen oder entfernen. Sie können Ihre Expositionsergebnisse mit der Dropdownliste Gruppieren nach gruppieren. Sie können Ihre Expositionsergebnisse auch mit dem Schnellfilter-Menü filtern.

Einzelheiten zu den Expositionsergebnissen

Sie können sich viele Details zu einem Expositionsergebnis ansehen. In der Security Hub Hub-Konsole sind diese Details auf mehrere Tabs aufgeteilt. Die Registerkarte „Übersicht“ bietet einen Überblick über die Ergebnisse der Sicherheitslücke. Auf der Registerkarte Merkmale sind die Merkmale und Signale aufgeführt, die mit einem Expositionsergebnis verknüpft sind. Die Registerkarte Ressourcen enthält Details zu den Ressourcen und Ressourcen-Tags, die mit einem Expositionsergebnis verknüpft sind. Die folgende Liste enthält Beschreibungen der Einzelheiten zu den Ergebnissen der Exposition.

- Titel des Befundes — Der Titel des Expositionsergebnisses.
- Schweregrad — Der Schweregrad des Expositionsergebnisses. Security Hub verwendet die Anzahl und Kombination von Merkmalen für eine Ressource, um den Schweregrad einer Risikofeststellung zu bestimmen. Der Schweregrad kann CRITICAL, HIGHMEDIUM, oder sein LOW. Security Hub veröffentlicht keine Risikopergebnisse mit einem Schweregrad von INFORMATIONAL. Sie können das Severity über die Security Hub Hub-Konsole oder mit dem [BatchUpdateFindingsV2API](#)-Vorgang aktualisieren.
- Beschreibung — Die Beschreibung des Expositionsergebnisses.
- Typ — Der Name des Typs der Risikoermittlung. Der Name könnte zum Beispiel etwa so aussehen Exposure/Potential Impact/Resource Hijacking.
- Konto — Die ID des Unternehmens AWS-Konto, in dem der Expositionsergebnis generiert wurde.
- Alter — Gibt an, wie lange der Expositionsergebnis aktiv ist.
- Erstellungszeit — Ein Zeitstempel, der angibt, wann der Expositionsergebnis erstellt wurde.
- Änderungszeit — Ein Zeitstempel, der angibt, wann das Expositionsergebnis zuletzt aktualisiert wurde.
- Region — Der AWS-Region Ort, an dem der Expositionsergebnis generiert wurde.
- Produktname — Der Name des Produkts, das zur Expositionsermittlung geführt hat.
- Firmenname — Der Name des Unternehmens, das die Risikofeststellung erstellt hat.

- Name der Aktivität — Der Name der Aktivität.
- Status — Der Status dieses Expositionsergebnisses.
- Fund-ID — Eine eindeutige Kennung, die mit dem Expositionsergebnis verknüpft ist.
- Potenzieller Angriffspfad (nur Konsole) — Eine interaktive Visualisierung zeigt, wie potenzielle Angreifer auf Ressourcen zugreifen und die Kontrolle darüber übernehmen können, die mit der Entdeckung einer Sicherheitslücke verknüpft sind. Weitere Informationen finden Sie unter [Gefährdungen in Security Hub mit dem Diagramm des potenziellen Angriffspfads anzeigen](#).
- Merkmale — Identifiziert Merkmalstypen und Merkmalstitel, die mit dem Expositionsergebnis verknüpft sind. In der Security Hub Hub-Konsole können Sie Eigenschaften nach Merkmalstyp oder Signal anzeigen. Auf diese Weise können Sie wichtige Ergebnisse im Zusammenhang mit der jeweiligen Exposition analysieren.
- Ressourcen — Identifiziert die Ressource, die mit dem Expositionsergebnis verknüpft ist.

Überprüfung der Einzelheiten der Expositionsergebnisse

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

In diesem Thema wird beschrieben, wie Sie Details zu Risikoergebnissen in der Security Hub Hub-Konsole und mit der API überprüfen können.

Details zu einer Risikofeststellung in der Security Hub Hub-Konsole überprüfen

So zeigen Sie Details zu einer Risikofeststellung in der Security Hub Hub-Konsole an

1. Melden Sie sich mit Ihren Anmeldeinformationen an und öffnen Sie die Security Hub Hub-Konsole unter <https://console.aws.amazon.com/securityhub/v2/home? region=us-ost-1>.
2. Wählen Sie im Navigationsbereich die Option Exposures aus.
3. Wählen Sie ein Risikoergebnis aus, dessen Details Sie anzeigen möchten.

Überprüfen Sie die Details zu einem Risikoergebnis mit der API

Sie können die Ergebnisse zur Exposition mit der [GetFindingsV2](#)API oder mit der `awscli` überprüfen. Sie können die Ergebnisse mit dem `FindingProviderFieldsTypes` Parameter und

durch Angabe des Filterwerts filtern, Exposure/EC2 wenn Sie nur Expositionsergebnisse für EC2 Instances zurückgeben möchten. Sie können nach anderen Feldern filtern, um die Ergebnisse einzugrenzen.

-Beispielbefehl

Im Folgenden finden Sie ein AWS CLI Beispiel, mit dem die 10 zuletzt generierten Expositionsergebnisse in Ihrem Konto abgerufen werden. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
aws securityhub get-findings-v2 \
    --max-results '10' \
    --filter '{"CompositeFilters": [{"StringFilters":
[{"FieldName":"finding_info.title","Filter":
{"Value":"GuardDuty","Comparison":"PREFIX"}} ]}]}'
```

Behebung von Risikoprüfungen

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

In den Themen in diesem Abschnitt werden die Risiken einer Problembehebung für verschiedene AWS-Services Bereiche beschrieben.

Das Remediation Feld [des OCSF-Formats](#) enthält zwei Felder: remediation und. references

```
"Remediation": {
  "Recommendation": {
    "remediation":{"desc":"String",
    "references":["string array"]}
  }
},
```

Note

Die in den folgenden Abschnitten enthaltenen Hinweise zur Problembehebung erfordern möglicherweise zusätzliche Konsultationen in anderen AWS Ressourcen.

Behebung von Risiken für DynamoDB-Tabellen

AWS Security Hub kann Risikopergebnisse für DynamoDB-Tabellen generieren.

Auf der Security Hub Hub-Konsole sind die DynamoDB-Tabelle, die an einer Risikofeststellung beteiligt war, und ihre identifizierenden Informationen im Abschnitt Ressourcen der Ergebnisdetails aufgeführt. Programmgesteuert können Sie Ressourcendetails mithilfe der [GetFindingsV2](#) Security Hub Hub-API abrufen.

Nachdem Sie die Ressource identifiziert haben, die an einer Risikofeststellung beteiligt war, können Sie die Ressource löschen, falls Sie sie nicht benötigen. Durch das Löschen einer nicht benötigten Ressource können Sie Ihr Expositionsprofil und Ihre AWS Kosten reduzieren. Wenn es sich bei der Ressource um eine wichtige Ressource handelt, befolgen Sie diese empfohlenen Abhilfemaßnahmen, um das Risiko zu minimieren. Die Themen zur Problembehebung sind nach der Art des Merkmals unterteilt.

Ein einziger Risikobefund umfasst Probleme, die in mehreren Problembehebungsthemen identifiziert wurden. Umgekehrt können Sie mit einem Problembehebungsproblem umgehen und dessen Schweregrad verringern, indem Sie sich mit nur einem Problembehebungsthema befassen. Ihr Ansatz zur Risikominderung hängt von den Anforderungen und der Arbeitsbelastung Ihres Unternehmens ab.

Note

Die in diesem Thema enthaltenen Hinweise zur Problembehebung erfordern möglicherweise zusätzliche Informationen in anderen Ressourcen. AWS

Inhalt

- [Merkmale von Fehlkonfigurationen in DynamoDB](#)
 - [Für die DynamoDB-Tabelle ist point-in-time die Wiederherstellung deaktiviert](#)
 - [Die DynamoDB-Tabelle ist nicht durch einen Backup-Plan abgedeckt](#)
 - [Für die DynamoDB-Tabelle ist der Löschschutz deaktiviert](#)

Merkmale von Fehlkonfigurationen in DynamoDB

Im Folgenden werden die Merkmale der Fehlkonfiguration und die Schritte zur Behebung von DynamoDB-Tabellen beschrieben.

Für die DynamoDB-Tabelle ist point-in-time die Wiederherstellung deaktiviert

DynamoDB-Wiederherstellung point-in-time aktivieren

point-in-timeDynamoDB-Wiederherstellung bietet kontinuierliche automatisierte Backups für Ihre DynamoDB-Tabellendaten. Informationen zum Wiederherstellen einer DynamoDB-Tabelle auf einen bestimmten Zeitpunkt finden Sie unter [Wiederherstellen einer DynamoDB-Tabelle auf einen bestimmten Zeitpunkt im Amazon DynamoDB](#) DynamoDB-Benutzerhandbuch.

Die DynamoDB-Tabelle ist nicht durch einen Backup-Plan abgedeckt

AWS Backup bietet einen zentralisierten Service zur Konfiguration, Verwaltung und Automatisierung von Backups für verschiedene AWS Dienste, einschließlich DynamoDB. Ohne einen Backup-Plan fehlen Ihrer Tabelle geplante, automatisierte Backups mit anpassbaren Aufbewahrungszeiträumen, was zu erheblichen Sicherheitsrisiken führt. Ein Angreifer könnte Ihre Tabellendaten in böswilliger Absicht beschädigen oder löschen. Ohne ordnungsgemäße Backups steht Ihnen möglicherweise keine Wiederherstellungsoption außerhalb des Point-in-Time Wiederherstellungsfensters zur Verfügung (falls aktiviert), was möglicherweise zu einem dauerhaften Datenverlust führen kann. Gemäß den Best Practices für den Datenschutz empfehlen wir, Ihre DynamoDB-Tabellen mit einem Backup-Plan abzudecken.

Erstellen Sie einen Backup-Plan

Bevor Sie einen Backup-Plan erstellen, legen Sie eine angemessene Sicherungshäufigkeit und Aufbewahrungsfristen für Ihre Daten fest. Informationen zum Erstellen eines Backup-Plans finden Sie unter [Zuweisen von Ressourcen zu einem Backup-Plan](#) im Amazon DynamoDB DynamoDB-Benutzerhandbuch.

Für die DynamoDB-Tabelle ist der Löschschutz deaktiviert

Der Löschschutz verhindert das versehentliche Löschen von DynamoDB-Tabellen. Wenn der Löschschutz deaktiviert ist, sind DynamoDB-Tabellen anfällig für unbeabsichtigtes Löschen durch Konsolenaktionen, API-Aufrufe, CLI-Befehle oder automatisierte Prozesse. Dadurch kann Ihre AWS Umgebung einem Datenverlust ausgesetzt sein, da eine nicht autorisierte Entität mit Zugriff auf Ihre AWS Umgebung absichtlich Tabellen löschen könnte, was zu Betriebsunterbrechungen und dauerhaftem Datenverlust führen könnte. Gemäß den Best Practices für den Datenschutz empfehlen wir, den Datenschutz für DynamoDB-Tabellen zu aktivieren.

Löschschutz aktivieren

Wenn Sie mehrere Tabellen verwalten, sollten Sie erwägen, die Tabelleneigenschaften in großen Mengen AWS CloudFormation zu aktualisieren. Sie können Ihre AWS CloudFormation Vorlagen so ändern, dass sie `DeletionProtectionEnabled` Eigenschaften enthalten, und Ihre Stapel aktualisieren. Stellen Sie nach Abschluss der Korrektur sicher, dass der Löschschutz in der Dropdownliste Zusätzliche Informationen auf der Registerkarte Einstellungen der Tabelle aktiviert ist.

Behebung von Risiken für Instanzen EC2

AWS Security Hub kann Risikopergebnisse für Amazon Elastic Compute Cloud (EC2) -Instances generieren.

Auf der Security Hub Hub-Konsole werden die EC2 Instanz, die an einer Risikofeststellung beteiligt war, und ihre identifizierenden Informationen im Abschnitt Ressourcen der Ergebnisdetails aufgeführt. Programmgesteuert können Sie Ressourcendetails mithilfe der [GetFindingsV2](#) Security Hub Hub-API abrufen.

Nachdem Sie die Ressource identifiziert haben, die an einer Risikofeststellung beteiligt war, können Sie die Ressource löschen, falls Sie sie nicht benötigen. Durch das Löschen einer nicht benötigten Ressource können Sie Ihr Expositionsprofil und Ihre AWS Kosten reduzieren. Wenn es sich bei der Ressource um eine wichtige Ressource handelt, befolgen Sie diese empfohlenen Abhilfemaßnahmen, um das Risiko zu minimieren. Die Themen zur Problembehebung sind nach der Art des Merkmals unterteilt.

Ein einziger Risikobefund umfasst Probleme, die in mehreren Problembehebungsthemen identifiziert wurden. Umgekehrt können Sie mit einem Problembehebungsproblem umgehen und dessen Schweregrad verringern, indem Sie sich mit nur einem Problembehebungsthema befassen. Ihr Ansatz zur Risikominderung hängt von den Anforderungen und der Arbeitsbelastung Ihres Unternehmens ab.

Note

Die in diesem Thema enthaltenen Hinweise zur Problembehebung erfordern möglicherweise zusätzliche Informationen in anderen Ressourcen. AWS

Inhalt

- [Merkmale der Fehlkonfiguration von Instanzen EC2](#)
 - [Die EC2 Instanz ermöglicht den Zugriff auf IMDS mit Version 1](#)
 - [Die mit der EC2 Amazon-Instance verknüpfte IAM-Rolle hat eine administrative Zugriffsrichtlinie](#)

- [Die mit der EC2 Amazon-Instance verknüpfte IAM-Rolle hat eine Service-Admin-Richtlinie](#)
- [Die EC2 Amazon-Instance verfügt über eine Sicherheitsgruppe oder Netzwerk-ACL, die SSH- oder RDP-Zugriff ermöglicht](#)
- [Die EC2 Amazon-Instance hat eine offene Sicherheitsgruppe](#)
- [Die EC2 Amazon-Instance hat eine öffentliche IP-Adresse](#)
- [EC2 Erreichbarkeitsmerkmale für Instances](#)
 - [Die EC2 Instanz ist über das Internet erreichbar](#)
 - [Die EC2 Amazon-Instance ist innerhalb der Amazon VPC erreichbar](#)
- [Merkmale der Sicherheitslücke für EC2 Instances](#)
 - [EC2 Die Instanz weist Softwareschwachstellen auf, die über das Netzwerk ausgenutzt werden können und die Wahrscheinlichkeit einer Ausnutzung hoch ist](#)
 - [Die EC2 Amazon-Instance weist Softwareschwachstellen auf](#)

Merkmale der Fehlkonfiguration von Instanzen EC2

Im Folgenden finden Sie Merkmale von Fehlkonfigurationen für EC2 Instanzen und empfohlene Schritte zur Behebung.

Die EC2 Instanz ermöglicht den Zugriff auf IMDS mit Version 1

Instance-Metadaten sind Daten über Ihre EC2 Amazon-Instance, die Anwendungen verwenden können, um die laufende Instance zu konfigurieren oder zu verwalten. Der Instance-Metadaten-Service (IMDS) ist eine On-Instance-Komponente, die von Code auf der Instance verwendet wird, um sicher auf Instance-Metadaten zuzugreifen. Wenn IMDS nicht ordnungsgemäß gesichert ist, kann es zu einem potenziellen Angriffsvektor werden, da es Zugriff auf temporäre Anmeldeinformationen und andere sensible Konfigurationsdaten bietet. IMDSv2 bietet einen besseren Schutz vor Ausnutzung durch sitzungsorientierte Authentifizierung, die ein Sitzungstoken für Metadatenanfragen erfordert und die Sitzungsdauer begrenzt. Es wird AWS empfohlen, EC2 Amazon-Instances gemäß den Standardsicherheitsprinzipien so zu konfigurieren, dass sie verwendet IMDSv2 und deaktiviert IMDSv1 werden.

Testen Sie die Anwendungskompatibilität

Testen Sie Ihre Instance vor der Implementierung IMDSv2, um sicherzustellen, dass sie kompatibel mit ist IMDSv2. IMDSv1 Für einige Anwendungen oder Skripts sind möglicherweise Kernfunktionen erforderlich und eine zusätzliche Konfiguration erforderlich. Weitere Informationen zu Tools und

empfohlenen Pfaden zum Testen der Anwendungskompatibilität finden Sie unter [Übergang zur Verwendung von Instance Metadata Service Version 2](#) im Amazon Elastic Compute Cloud-Benutzerhandbuch.

Aktualisieren Sie die zu verwendende Instanz IMDSv2

Ändern Sie vorhandene Instanzen, die verwendet IMDSv2 werden sollen. Weitere Informationen finden Sie unter [Ändern von Instance-Metadaten-Optionen für bestehende Instances](#) im Amazon Elastic Compute Cloud-Benutzerhandbuch.

Updates auf Instances in einer Auto Scaling Scaling-Gruppe anwenden

Wenn Ihre Instance Teil einer Auto Scaling Scaling-Gruppe ist, aktualisieren Sie Ihre Startvorlage oder Startkonfiguration mit einer neuen Konfiguration und führen Sie eine Instance-Aktualisierung durch.

Die mit der EC2 Amazon-Instance verknüpfte IAM-Rolle hat eine administrative Zugriffsrichtlinie

Administrative Zugriffsrichtlinien bieten EC2 Amazon-Instances umfassende Berechtigungen AWS-Services und Ressourcen. Diese Richtlinien beinhalten in der Regel Berechtigungen, die für die Instance-Funktionalität nicht erforderlich sind. Die Bereitstellung einer IAM-Identität mit einer administrativen Zugriffsrichtlinie für eine EC2 Amazon-Instance (anstelle der Mindestberechtigungen, die die Ihrem Instance-Profil zugeordnete Rolle benötigt) kann den Umfang eines Angriffs erhöhen, wenn die EC2 Amazon-Instance kompromittiert wird. Wenn eine Instance kompromittiert wird, könnten Angreifer diese übermäßigen Berechtigungen nutzen, um sich seitlich in Ihrer Umgebung zu bewegen, auf Daten zuzugreifen oder Ressourcen zu manipulieren. Gemäß den Standardsicherheitsprinzipien empfehlen wir, die geringsten Rechte zu gewähren, d. h., Sie gewähren nur die Berechtigungen, die für die Ausführung einer Aufgabe erforderlich sind.

Überprüfen und identifizieren Sie die Verwaltungsrichtlinien

Suchen Sie im IAM-Dashboard nach der Rolle mit dem Rollennamen. Überprüfen Sie die der IAM-Rolle beigefügte Berechtigungsrichtlinie. Wenn es sich bei der Richtlinie um eine AWS verwaltete Richtlinie handelt, suchen Sie nach `AdministratorAccess` oder `IAMFullAccess`. Andernfalls suchen Sie im Richtliniendokument nach Aussagen mit `"Effect": "Allow"`, `"Action": "*"`, und `"Resource": "*"`.

Implementieren des Zugriffs mit geringsten Berechtigungen

Ersetzen Sie Verwaltungsrichtlinien durch Richtlinien, die nur die spezifischen Berechtigungen gewähren, die für das Funktionieren der Instanz erforderlich sind. Weitere Informationen zu

bewährten Sicherheitsmethoden für IAM-Rollen finden Sie unter [Anwenden von Berechtigungen mit den geringsten Rechten](#) im Abschnitt Bewährte Sicherheitsmethoden im Benutzerhandbuch.AWS Identity and Access Management Um unnötige Berechtigungen zu identifizieren, können Sie den IAM Access Analyzer verwenden, um zu erfahren, wie Sie Ihre Richtlinie auf der Grundlage des Zugriffsverlaufs ändern können. Weitere Informationen finden Sie im AWS Identity and Access Management Benutzerhandbuch unter [Ergebnisse für externen und ungenutzten Zugriff](#). Alternativ können Sie eine neue IAM-Rolle erstellen, um zu vermeiden, dass andere Anwendungen, die die bestehende Rolle verwenden, beeinträchtigt werden. Erstellen Sie in diesem Szenario eine neue IAM-Rolle und ordnen Sie dann die neue IAM-Rolle der Instance zu. Anweisungen zum Ersetzen einer IAM-Rolle für eine Instance finden Sie unter [Eine IAM-Rolle an eine Instance anhängen](#) im Amazon Elastic Compute Cloud-Benutzerhandbuch.

Überlegungen zur sicheren Konfiguration

Wenn für die Instanz Administratorberechtigungen auf Service-Ebene erforderlich sind, sollten Sie die Implementierung dieser zusätzlichen Sicherheitskontrollen in Betracht ziehen, um das Risiko zu minimieren:

- Überlegungen zur sicheren Konfiguration
 - Multi-Faktor-Authentifizierung (MFA) — MFA fügt eine zusätzliche Sicherheitsebene hinzu, da eine zusätzliche Form der Authentifizierung erforderlich ist. Dies hilft, unbefugten Zugriff zu verhindern, selbst wenn Anmeldeinformationen kompromittiert werden. Weitere Informationen finden Sie im AWS Identity and Access Management Benutzerhandbuch unter [Multi-Faktor-Authentifizierung \(MFA\) erforderlich](#).
 - IAM-Bedingungen — Durch die Einrichtung von Bedingungelementen können Sie anhand von Faktoren wie Quell-IP oder MFA-Alter einschränken, wann und wie Administratorberechtigungen verwendet werden können. Weitere Informationen finden Sie im Benutzerhandbuch unter [Verwenden von Bedingungen in IAM-Richtlinien, um den Zugriff weiter einzuschränken](#).AWS Identity and Access Management
 - Berechtigungsgrenzen — Berechtigungsgrenzen legen die maximale Anzahl von Berechtigungen fest, die eine Rolle haben kann, und bieten so Richtlinien für Rollen mit Administratorzugriff. Weitere Informationen finden Sie im Benutzerhandbuch unter [Verwenden von Berechtigungsgrenzen, um die Rechteverwaltung innerhalb eines Kontos zu delegieren](#).AWS Identity and Access Management

Updates auf Instances in einer Auto Scaling-Gruppe anwenden

Aktualisieren Sie für EC2 Amazon-Instances in einer AWS Auto Scaling-Gruppe die Startvorlage oder die Startkonfiguration mit dem neuen Instance-Profil und führen Sie eine Instance-Aktualisierung durch. Informationen zum Aktualisieren einer Startvorlage finden Sie unter [Ändern einer Startvorlage \(Startvorlagenversionen verwalten\)](#) im Amazon Elastic Compute Cloud-Benutzerhandbuch. Weitere Informationen finden Sie unter [Verwenden einer Instanzaktualisierung, um Instances in einer Auto Scaling Scaling-Gruppe zu aktualisieren](#). Weitere Informationen zur Verwendung von IAM-Rollen mit Auto Scaling Scaling-Gruppen finden Sie unter [IAM-Rolle für Anwendungen, die auf EC2 Amazon-Instances ausgeführt werden, im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch](#).

Die mit der EC2 Amazon-Instance verknüpfte IAM-Rolle hat eine Service-Admin-Richtlinie

Richtlinien für den Servicezugriff gewähren EC2 Amazon-Instances umfassende Berechtigungen für AWS Dienste und Ressourcen. Diese Richtlinien beinhalten in der Regel Berechtigungen, die für die Instance-Funktionalität nicht erforderlich sind. Die Bereitstellung einer IAM-Identität mit einer administrativen Zugriffsrichtlinie für eine EC2 Amazon-Instance anstelle der Mindestberechtigungen, die die Ihrem Instance-Profil zugeordnete Rolle benötigt, kann den Umfang eines Angriffs erhöhen, wenn eine Instance kompromittiert wird. Gemäß den Standardsicherheitsprinzipien empfehlen wir, die geringsten Rechte zu gewähren, was bedeutet, dass Sie nur die Berechtigungen gewähren, die für die Ausführung einer Aufgabe erforderlich sind.

Überprüfen und identifizieren Sie die Verwaltungsrichtlinien

Suchen Sie im IAM-Dashboard nach der Rolle mit dem Rollennamen. Überprüfen Sie die der IAM-Rolle beigefügte Berechtigungsrichtlinie. Wenn es sich bei der Richtlinie um eine AWS verwaltete Richtlinie handelt, suchen Sie nach `AdministratorAccess` oder `IAMFullAccess`. Andernfalls suchen Sie im Richtliniendokument nach Aussagen mit `"Effect": "Allow"`, `"Action": "*"`, und `"Resource": "*"`.

Implementieren des Zugriffs mit geringsten Berechtigungen

Ersetzen Sie Dienstadministratorrichtlinien durch solche, die nur die spezifischen Berechtigungen gewähren, die für das Funktionieren der Instanz erforderlich sind. Weitere Informationen zu bewährten Sicherheitsmethoden für IAM-Rollen finden Sie unter [Anwenden von Berechtigungen mit den geringsten Rechten](#) im Abschnitt Bewährte Sicherheitsmethoden im Benutzerhandbuch.AWS Identity and Access Management Um unnötige Berechtigungen zu identifizieren, können Sie den IAM Access Analyzer verwenden, um zu erfahren, wie Sie Ihre Richtlinie auf der Grundlage des Zugriffsverlaufs ändern können. Weitere Informationen finden Sie im AWS Identity and Access Management Benutzerhandbuch unter [Ergebnisse für externen und ungenutzten Zugriff](#). Alternativ können Sie eine neue IAM-Rolle erstellen, um zu vermeiden, dass sich dies auf andere

Anwendungen auswirkt, die die vorhandene Rolle verwenden. Erstellen Sie in diesem Szenario eine neue IAM-Rolle und ordnen Sie dann die neue IAM-Rolle der Instance zu. Informationen zum Ersetzen einer IAM-Rolle für eine Instance finden Sie unter [Anhängen einer IAM-Rolle an eine Instance](#) im Amazon Elastic Compute Cloud-Benutzerhandbuch.

Überlegungen zur sicheren Konfiguration

Wenn für die Instanz Administratorberechtigungen auf Service-Ebene erforderlich sind, sollten Sie die Implementierung dieser zusätzlichen Sicherheitskontrollen in Betracht ziehen, um das Risiko zu minimieren:

Überlegungen zur sicheren Konfiguration

Wenn für die Instanz Administratorberechtigungen auf Service-Ebene erforderlich sind, sollten Sie die Implementierung dieser zusätzlichen Sicherheitskontrollen in Betracht ziehen, um das Risiko zu minimieren:

- Multi-Faktor-Authentifizierung (MFA) — MFA fügt eine zusätzliche Sicherheitsebene hinzu, da eine zusätzliche Form der Authentifizierung erforderlich ist. Dies hilft, unbefugten Zugriff zu verhindern, selbst wenn Anmeldeinformationen kompromittiert werden. Weitere Informationen finden Sie im AWS Identity and Access Management Benutzerhandbuch unter [Multi-Faktor-Authentifizierung \(MFA\) erforderlich](#).
- IAM-Bedingungen — Durch die Einrichtung von Bedingungelementen können Sie anhand von Faktoren wie Quell-IP oder MFA-Alter einschränken, wann und wie Administratorberechtigungen verwendet werden können. Weitere Informationen finden Sie im Benutzerhandbuch unter [Verwenden von Bedingungen in IAM-Richtlinien, um den Zugriff weiter einzuschränken](#).AWS Identity and Access Management
- Berechtigungsgrenzen — Berechtigungsgrenzen legen die maximale Anzahl von Berechtigungen fest, die eine Rolle haben kann, und bieten so Richtlinien für Rollen mit Administratorzugriff. Weitere Informationen finden Sie im Benutzerhandbuch unter [Verwenden von Berechtigungsgrenzen, um die Rechteverwaltung innerhalb eines Kontos zu delegieren](#).AWS Identity and Access Management

Updates auf Instanzen in der Auto Scaling Scaling-Gruppe anwenden

Aktualisieren Sie für EC2 Amazon-Instances in einer AWS Auto Scaling-Gruppe die Startvorlage oder die Startkonfiguration mit dem neuen Instance-Profil und führen Sie eine Instance-Aktualisierung durch. Informationen zum Aktualisieren einer Startvorlage finden Sie unter [Ändern einer Startvorlage](#)

([Startvorlagenversionen verwalten](#)) im Amazon Elastic Compute Cloud-Benutzerhandbuch. Weitere Informationen finden Sie unter [Verwenden einer Instanzaktualisierung, um Instances in einer Auto Scaling Scaling-Gruppe zu aktualisieren](#). Weitere Informationen zur Verwendung von IAM-Rollen mit Auto Scaling Scaling-Gruppen finden Sie unter [IAM-Rolle für Anwendungen, die auf EC2 Amazon-Instances ausgeführt werden, im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch](#).

Die EC2 Amazon-Instance verfügt über eine Sicherheitsgruppe oder Netzwerk-ACL, die SSH- oder RDP-Zugriff ermöglicht

Fernzugriffsprotokolle wie SSH und RDP ermöglichen es Benutzern, von externen Standorten aus eine Verbindung zu EC2 Amazon-Instances herzustellen und diese zu verwalten. Wenn Sicherheitsgruppen den uneingeschränkten Zugriff auf diese Protokolle aus dem Internet zulassen, vergrößern sie die Angriffsfläche Ihrer EC2 Amazon-Instances, indem sie den Internetzugriff auf Ihre Instance ermöglichen. Es wird AWS empfohlen, den Fernzugriff auf bestimmte, vertrauenswürdige IP-Adressen oder Bereiche zu beschränken.

1. Ändern Sie die Regeln für Sicherheitsgruppen

Beschränken Sie den Zugriff auf Ihre EC2 Amazon-Instances auf bestimmte vertrauenswürdige IP-Adressen. Beschränken Sie den SSH- und RDP-Zugriff auf bestimmte vertrauenswürdige IP-Adressen oder verwenden Sie die CIDR-Notation, um IP-Bereiche anzugeben (z. B. 198.168.1.0/24). Informationen zum Ändern von Sicherheitsgruppenregeln finden [Sie unter Sicherheitsgruppenregeln konfigurieren](#) im Amazon Elastic Compute Cloud-Benutzerhandbuch.

Die EC2 Amazon-Instance hat eine offene Sicherheitsgruppe

Sicherheitsgruppen dienen als virtuelle Firewalls für Ihre EC2 Amazon-Instances, um den eingehenden und ausgehenden Datenverkehr zu kontrollieren. Offene Sicherheitsgruppen, die uneingeschränkten Zugriff von jeder IP-Adresse aus ermöglichen, können Ihre Instances unbefugten Zugriffen aussetzen. Es wird AWS empfohlen, den Zugriff von Sicherheitsgruppen auf bestimmte IP-Adressen und Ports gemäß den Standardsicherheitsprinzipien zu beschränken.

Überprüfen Sie die Sicherheitsgruppenregeln und bewerten Sie die aktuelle Konfiguration

Prüfen Sie, welche Ports offen und von weiten IP-Bereichen aus zugänglich sind, z. (0.0.0.0/0 or ::/0) B. Anweisungen zum Anzeigen von Sicherheitsgruppendetails finden Sie [DescribeSecurityGroups](#) in der API-Referenz zum Porting Assistant for .NET.

Ändern Sie die Regeln für Sicherheitsgruppen

Ändern Sie Ihre Sicherheitsgruppenregeln, um den Zugriff auf bestimmte vertrauenswürdige IP-Adressen oder Bereiche einzuschränken. Denken Sie bei der Aktualisierung Ihrer Sicherheitsgruppenregeln darüber nach, die Zugriffsanforderungen für verschiedene Netzwerksegmente zu trennen, indem Sie Regeln für jeden erforderlichen Quell-IP-Bereich erstellen oder den Zugriff auf bestimmte Ports einschränken. Informationen zum Ändern von Sicherheitsgruppenregeln finden [Sie unter Sicherheitsgruppenregeln konfigurieren](#) im EC2 Amazon-Benutzerhandbuch.

Die EC2 Amazon-Instance hat eine öffentliche IP-Adresse

EC2 Amazon-Instances mit öffentlichen IP-Adressen sind öffentlich über das Internet zugänglich. Öffentliche IP-Adressen sind zwar manchmal für Instances erforderlich, die Dienste für externe Kunden bereitstellen, dies kann jedoch als potenzieller Angriff auf nicht autorisierte Principals genutzt werden. Es wird AWS empfohlen, die Offenlegung von Ressourcen durch die Öffentlichkeit so gering wie möglich zu halten.

Verschieben Sie die Instance in ein privates Subnetz

Wenn die Instance keinen direkten Internetzugang benötigt, sollten Sie erwägen, sie in ein privates Subnetz innerhalb Ihrer VPC zu verschieben. Dadurch wird die öffentliche IP-Adresse entfernt und es kann weiterhin mit anderen Ressourcen innerhalb Ihrer VPC kommunizieren. Weitere Informationen finden Sie unter [Wie verschiebe ich meine EC2 Amazon-Instance in ein anderes Subnetz, eine Availability Zone oder eine VPC?](#) im AWS Knowledge Center.

Konfigurieren Sie Instanzen so, dass sie ohne öffentliche IP-Adressen gestartet werden

Wenn die Instance in einem öffentlichen Subnetz gestartet wurde, für das keine öffentlichen IP-Adressen erforderlich sind, kann die Startkonfiguration geändert werden, um die automatische Zuweisung von öffentlichen IP-Adressen zu verhindern. Dies kann auf Subnetzebene oder beim Starten einzelner Instances deaktiviert werden. Weitere Informationen finden Sie unter [Ändern der IP-Adressierungsattribute Ihres Subnetzes](#) im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch und unter [Amazon Amazon EC2instance IP-Adressierung](#) im Amazon Elastic Compute Cloud-Benutzerhandbuch.

Alternative Zugriffsmethoden

Erwägen Sie die folgenden Optionen für alternative Zugriffsmethoden:

- Verwenden Sie ein NAT-Gateway für ausgehende Internetkonnektivität —

Für Instanzen in privaten Subnetzen, die Zugriff auf das Internet benötigen (z. B. zum Herunterladen von Updates), sollten Sie die Verwendung eines NAT-Gateways in Betracht ziehen, anstatt eine öffentliche IP-Adresse zuzuweisen. Ein NAT-Gateway ermöglicht es Instances in privaten Subnetzen, ausgehende Verbindungen zum Internet zu initiieren und gleichzeitig eingehende Verbindungen aus dem Internet zu verhindern. Weitere Informationen finden Sie unter [NAT-Gateways](#) im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

- Elastic Load Balancing verwenden — Für Instances, auf denen Webanwendungen ausgeführt werden, sollten Sie die Verwendung eines Elastic Load Balancer (LB) in Betracht ziehen. LBs kann so konfiguriert werden, dass Ihre Instances in privaten Subnetzen ausgeführt werden können, während der LB in einem öffentlichen Subnetz läuft und den Internetverkehr abwickelt. Weitere Informationen finden Sie unter Was ist Elastic Load Balancing? im AWS ELB-Benutzerhandbuch. Anleitungen zur Auswahl einer Stickiness-Strategie für Ihren LB finden Sie unter [Load Balancer-Subnetze](#) in AWS Prescriptive Guidance.

EC2 Erreichbarkeitsmerkmale für Instances

Im Folgenden finden Sie Merkmale der Erreichbarkeit für EC2 Instanzen und empfohlene Schritte zur Behebung.

Die EC2 Instanz ist über das Internet erreichbar

EC2 Amazon-Instances mit Ports, die vom Internet aus über ein Internet-Gateway (einschließlich Instances hinter Application Load Balancers oder Classic Load Balancers), eine VPC-Peering-Verbindung oder ein virtuelles VPN-Gateway erreichbar sind, können Ihre Instance dem Internet aussetzen. Gemäß den Standardsicherheitsprinzipien empfehlen wir die Implementierung von Netzwerkzugriffskontrollen mit geringsten Rechten, indem eingehender Datenverkehr auf die erforderlichen Quellen und Ports beschränkt wird.

Sicherheitsgruppenregeln ändern oder entfernen

Öffnen Sie auf der Registerkarte Ressourcen die Ressource für die EC2 Amazon-Sicherheitsgruppe. Prüfen Sie, ob ein Internetzugang erforderlich ist, damit die Instance funktioniert. Ändern oder entfernen Sie Sicherheitsgruppenregeln für eingehenden Datenverkehr, die uneingeschränkten Zugriff ermöglichen (0.0.0.0/0oder: :/0). Implementieren Sie restriktivere Regeln, die auf bestimmten IP-Bereichen oder Sicherheitsgruppen basieren. Wenn ein eingeschränkter öffentlicher Zugriff erforderlich ist, beschränken Sie den Zugriff auf bestimmte Ports und Protokolle, die für die Funktion der Instanz erforderlich sind. Anweisungen zur Verwaltung von Sicherheitsgruppenregeln finden [Sie unter Sicherheitsgruppenregeln konfigurieren](#) im EC2 Amazon-Benutzerhandbuch.

Netzwerk aktualisieren ACLs

Überprüfen und ändern Sie die Netzwerkzugriffskontrolllisten (ACLs), die dem Subnetz der Instanz zugeordnet sind. Stellen Sie sicher, dass die ACL-Einstellungen mit den Änderungen der Sicherheitsgruppe übereinstimmen und nicht unbeabsichtigt öffentlichen Zugriff zulassen. Anweisungen zum Ändern des Netzwerks ACLs finden Sie unter [Work with network ACLs](#) im Amazon VPC-Benutzerhandbuch.

Alternative Zugriffsmethoden

Erwägen Sie die folgenden Optionen für alternative Zugriffsmethoden:

- Verwenden Sie das NAT-Gateway für ausgehende Internetkonnektivität — Für Instances in privaten Subnetzen, die Zugriff auf das Internet benötigen (z. B. um Updates herunterzuladen), sollten Sie ein NAT-Gateway verwenden, anstatt eine öffentliche IP-Adresse zuzuweisen. Ein NAT-Gateway ermöglicht es Instances in privaten Subnetzen, ausgehende Verbindungen zum Internet zu initiieren und gleichzeitig eingehende Verbindungen aus dem Internet zu verhindern.
- Verwenden Sie Systems Manager Session Manager — Session Manager bietet sicheren Shell-Zugriff auf Ihre EC2 Amazon-Instances, ohne dass eingehende Ports erforderlich sind, SSH-Schlüssel verwaltet oder Bastion-Hosts verwaltet werden müssen.
- Verwenden Sie WAF und Elastic Load Balancing oder Application Load Balancer — Für Instances, auf denen Webanwendungen ausgeführt werden, sollten Sie erwägen, einen LB in Kombination mit einer AWS Web Application Firewall (WAF) zu verwenden. LBs kann so konfiguriert werden, dass Ihre Instances in privaten Subnetzen ausgeführt werden können, während der LB in einem öffentlichen Subnetz läuft und den Internetverkehr abwickelt. Das Hinzufügen einer WAF zu Ihrem Load Balancer bietet zusätzlichen Schutz vor Web-Exploits und Bots.

Die EC2 Amazon-Instance ist innerhalb der Amazon VPC erreichbar

Mit Amazon Virtual Private Cloud (Amazon VPC) können Sie AWS Ressourcen in einem definierten virtuellen Netzwerk starten. Amazon VPC-Netzwerkkonfigurationen, die uneingeschränkten Zugriff zwischen Instances ermöglichen, können den Umfang eines Angriffs erhöhen, wenn eine Instance kompromittiert wird. Es wird AWS empfohlen, Netzwerksegmentierung und Zugriffskontrollen mit geringsten Rechten auf Subnetz- und Sicherheitsgruppenebene zu implementieren.

Überprüfen Sie die Netzwerkverbindungsmuster von Amazon VPC

Identifizieren Sie in der Risikofeststellung die Sicherheitsgruppen-ID im ARN. Identifizieren Sie, welche Instances miteinander kommunizieren müssen und über welche Ports. Sie können Amazon

VPC Flow Logs verwenden, um bestehende Datenverkehrsmuster in Ihrer Amazon VPC zu analysieren, um festzustellen, welche Ports verwendet werden.

Ändern Sie die Regeln für Sicherheitsgruppen

Ändern Sie Ihre Sicherheitsgruppenregeln, um den Zugriff auf bestimmte vertrauenswürdige IP-Adressen oder Bereiche einzuschränken. Anstatt beispielsweise den gesamten Datenverkehr aus dem gesamten VPC-CIDR-Bereich (z. B. 10.0.0.0/16) zuzulassen, sollten Sie den Zugriff auf bestimmte Sicherheitsgruppen oder IP-Bereiche einschränken. Denken Sie bei der Aktualisierung Ihrer Sicherheitsgruppenregeln darüber nach, die Zugriffsanforderungen für verschiedene Netzwerksegmente zu trennen, indem Sie Regeln für jeden erforderlichen Quell-IP-Bereich erstellen oder den Zugriff auf bestimmte Ports einschränken. Informationen zum Ändern von Sicherheitsgruppenregeln finden Sie unter [Sicherheitsgruppenregeln konfigurieren](#) im EC2 Amazon-Benutzerhandbuch.

Erwägen Sie, Ihre Amazon VPC-Ressourcen auf der Grundlage von Sicherheitsanforderungen oder Funktionen in Subnetze zu organisieren. Platzieren Sie beispielsweise Webserver und Datenbankserver in separaten Subnetzen. Weitere Informationen finden Sie unter [Subnetze für Ihre VPC](#) im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

Konfigurieren Sie das Netzwerk ACLs für den Schutz auf Subnetzebene

Network Access Control Lists (NACLs) bieten eine zusätzliche Sicherheitsebene auf Subnetzebene. Im Gegensatz zu Sicherheitsgruppen NACLs sind sie zustandslos und erfordern, dass sowohl eingehende als auch ausgehende Regeln explizit definiert werden. Weitere Informationen finden Sie unter [Steuern des Subnetzverkehrs mit Netzwerkzugriffskontrolllisten](#) im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

Weitere Überlegungen

Beachten Sie Folgendes, wenn Sie den Zugriff auf Ihre Amazon VPC einschränken

- **Transit Gateway oder Amazon VPC Peering mit restriktivem Routing** — Wenn Ihre Architektur mehrere verwendet, VPCs die kommunizieren müssen, sollten Sie die Verwendung von AWS Transit Gateway und Amazon VPC Peering in Betracht ziehen, um Konnektivität zwischen Amazon bereitzustellen und VPCs gleichzeitig zu kontrollieren, welche Subnetze miteinander kommunizieren können. Weitere Informationen finden [Sie unter Erste Schritte mit der Verwendung von Amazon VPC Transit Gateways](#) und [VPC-Peering-Verbindungen](#).
- **Service-Endpunkte und private Links** — Amazon VPC-Endpunkte können verwendet werden, um den Datenverkehr innerhalb des AWS Netzwerks zu halten und mit AWS Ressourcen statt

über das Internet zu kommunizieren. Dies reduziert den Bedarf an direkter Konnektivität zwischen Instances, die auf dieselben Dienste zugreifen. Informationen zu VPC-Endpunkten finden Sie unter [Was sind Amazon VPC-Endpunkte?](#) im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch. Für die Konnektivität zu Diensten, die in anderen Amazon-Ländern gehostet werden VPCs, sollten Sie die Verwendung von in Betracht ziehen AWS PrivateLink.

Merkmale der Sicherheitslücke für EC2 Instances

Im Folgenden finden Sie die Merkmale der Sicherheitslücken für EC2 Instanzen und empfohlene Schritte zur Behebung.

EC2 Die Instanz weist Softwareschwachstellen auf, die über das Netzwerk ausgenutzt werden können und die Wahrscheinlichkeit einer Ausnutzung hoch ist

Softwarepakete, die auf EC2 Instanzen installiert sind, können häufig anfälligen Sicherheitslücken () ausgesetzt sein. CVEs Kritische CVEs Sicherheitsrisiken stellen erhebliche Sicherheitsrisiken für Ihre AWS Umgebung dar. Unbefugte Benutzer können diese ungepatchten Sicherheitslücken ausnutzen, um die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten zu gefährden oder auf andere Systeme zuzugreifen. Kritische Sicherheitslücken mit hoher Wahrscheinlichkeit stellen unmittelbare Sicherheitsbedrohungen dar, da Exploit-Code möglicherweise bereits öffentlich verfügbar ist und von Angreifern oder automatisierten Scan-Tools aktiv genutzt wird. Wir empfehlen, diese Sicherheitslücken zu patchen, um Ihre Instanz zu schützen.

Aktualisieren Sie die betroffenen Instanzen

Sehen Sie sich den Abschnitt Referenzen auf der Registerkarte Sicherheitslücke des Merkmals an. Die Herstellerdokumentation kann spezifische Anleitungen zur Problembehebung enthalten. Folgen Sie den entsprechenden Abhilfemaßnahmen anhand dieser allgemeinen Richtlinien:

Verwenden Sie Systems Manager Patch Manager, um Patches für Betriebssysteme und Anwendungen anzuwenden. Patch Manager unterstützt Sie bei der automatischen Auswahl und Bereitstellung von Betriebssystem- und Softwarepatches für große Gruppen von Instanzen. Wenn Sie Patch Manager nicht konfiguriert haben, aktualisieren Sie das Betriebssystem auf jeder betroffenen Instanz manuell.

Aktualisieren Sie die betroffenen Anwendungen gemäß den vom Hersteller empfohlenen Verfahren auf ihre neuesten sicheren Versionen. Um Anwendungsupdates über mehrere Instanzen hinweg zu verwalten, sollten Sie den Systems Manager State Manager verwenden, um Ihre Software in einem konsistenten Zustand zu halten. Wenn keine Updates verfügbar sind, sollten Sie erwägen,

die anfällige Anwendung zu entfernen oder zu deaktivieren, bis ein Patch veröffentlicht wird, oder Sie sollten andere Abhilfemaßnahmen ergreifen, z. B. den Netzwerkzugriff auf die Anwendung einschränken oder anfällige Funktionen deaktivieren.

Folgen Sie den spezifischen Empfehlungen zur Problembehebung im Ergebnis von Amazon Inspector. Dies kann das Ändern von Sicherheitsgruppenregeln, das Ändern von Instance-Konfigurationen oder das Anpassen von Anwendungseinstellungen beinhalten.

Prüfen Sie, ob die Instance Teil der Auto Scaling Group ist. AMI-Ersatz-Patches werden auf unveränderlichen Infrastrukturen durchgeführt, indem die AMI-ID aktualisiert wird, die für die Bereitstellung neuer EC2 Amazon-Instances in einer Auto Scaling Group konfiguriert ist. Wenn Sie ein custom/golden AMI verwenden, erstellen Sie eine Instance mit dem neuen AMI, passen Sie dann die Instance an und erstellen Sie ein neues goldenes AMI. Weitere Informationen finden Sie unter [Patching für AMI-Updates \(Verwendung von Patched AMIs für Auto Scaling Groups\)](#).

Überlegungen für die Zukunft

Um future Vorkommnisse zu verhindern, sollten Sie die Implementierung eines Vulnerability Management-Programms in Betracht ziehen. Amazon Inspector kann so konfiguriert werden, dass es automatisch CVEs nach Ihren Instances sucht. Amazon Inspector kann für automatische Problembehebungen auch in Security Hub integriert werden. Erwägen Sie die Implementierung eines regelmäßigen Patch-Zeitplans mithilfe von Systems Manager Maintenance Windows, um Unterbrechungen Ihrer Instanzen so gering wie möglich zu halten.

Die EC2 Amazon-Instance weist Softwareschwachstellen auf

Softwarepakete, die auf Amazon installiert sind, EC2instances können allgemeinen Sicherheitslücken und Gefahren ausgesetzt sein (CVEs). Bei nicht kritischen Sicherheitslücken CVEs handelt es sich um Sicherheitslücken mit geringerem Schweregrad oder geringerer Ausnutzbarkeit als kritische. CVEs Diese Sicherheitslücken stellen zwar ein geringeres unmittelbares Risiko dar, aber Angreifer können diese ungepatchten Sicherheitslücken dennoch ausnutzen, um die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten zu gefährden oder auf andere Systeme zuzugreifen. Befolgt bewährte Sicherheitsmethoden und AWS empfiehlt, diese Sicherheitslücken zu patchen, um Ihre Instance vor Angriffen zu schützen.

Aktualisieren Sie die betroffenen Instanzen

Verwenden Sie AWS Systems Manager Patch Manager, um Patches für Betriebssysteme anzuwenden. Patch Manager unterstützt Sie bei der automatischen Auswahl und Bereitstellung von

Betriebssystem- und Softwarepatches für große Gruppen von Instanzen. Wenn Sie Patch Manager nicht konfiguriert haben, aktualisieren Sie das Betriebssystem auf jeder betroffenen Instanz manuell.

Aktualisieren Sie die betroffenen Anwendungen gemäß den vom Hersteller empfohlenen Verfahren auf ihre neuesten sicheren Versionen. Um Anwendungsupdates über mehrere Instanzen hinweg zu verwalten, sollten Sie den AWS Systems Manager State Manager verwenden, um Ihre Software in einem konsistenten Zustand zu halten. Wenn keine Updates verfügbar sind, sollten Sie erwägen, die anfällige Anwendung zu entfernen oder zu deaktivieren, bis ein Patch veröffentlicht wird, oder Sie sollten andere Abhilfemaßnahmen ergreifen, z. B. den Netzwerkzugriff auf die Anwendung einschränken oder anfällige Funktionen deaktivieren.

Folgen Sie den spezifischen Empfehlungen zur Problembehebung im Ergebnis von Amazon Inspector. Dies kann das Ändern von Sicherheitsgruppenregeln, das Ändern von Instance-Konfigurationen oder das Anpassen der Anwendungseinstellungen beinhalten.

Prüfen Sie, ob die Instance Teil der Auto Scaling Group ist. AMI-Ersatz-Patches werden auf unveränderlichen Infrastrukturen durchgeführt, indem die AMI-ID aktualisiert wird, die für die Bereitstellung neuer EC2 Amazon-Instances in einer Auto Scaling Group konfiguriert ist. Wenn Sie ein custom/golden AMI verwenden, erstellen Sie eine Instance mit dem neuen AMI, passen Sie dann die Instance an und erstellen Sie ein neues goldenes AMI. Weitere Informationen finden Sie unter [Patching für AMI-Updates \(Verwendung von Patched AMIs für Auto Scaling Groups\)](#).

Überlegungen für die Zukunft

Um future Vorkommnisse zu verhindern, sollten Sie die Implementierung eines Vulnerability Management-Programms in Betracht ziehen. Amazon Inspector kann so konfiguriert werden, dass es automatisch CVEs nach Ihren Instances sucht. Amazon Inspector kann für automatische Problembehebungen auch in Security Hub integriert werden. Erwägen Sie die Implementierung eines regelmäßigen Patch-Zeitplans mithilfe von Systems Manager Maintenance Windows, um Unterbrechungen Ihrer Instanzen so gering wie möglich zu halten.

Behebung von Risiken für Amazon ECS-Services

AWS Security Hub kann Ergebnisse zur Gefährdung von Amazon Elastic Container Service (Amazon ECS) -Services generieren.

Der Amazon ECS-Service, der an einer Expositionsfeststellung beteiligt war, und seine identifizierenden Informationen sind im Abschnitt Ressourcen der Ergebnisdetails aufgeführt. Sie können diese Ressourcendetails auf der Security Hub Hub-Konsole oder programmgesteuert mithilfe der [GetFindingsV2](#) Security Hub Hub-API abrufen.

Nachdem Sie die Ressource identifiziert haben, die an einer Risikofeststellung beteiligt war, können Sie die Ressource löschen, wenn Sie sie nicht benötigen. Durch das Löschen einer nicht benötigten Ressource können Sie Ihr Expositionsprofil und Ihre AWS Kosten reduzieren. Wenn es sich bei der Ressource um eine wichtige Ressource handelt, befolgen Sie diese empfohlenen Abhilfemaßnahmen, um das Risiko zu minimieren. Die Themen zur Problembehebung sind nach der Art des Merkmals unterteilt.

Ein einziger Risikobefund umfasst Probleme, die in mehreren Problembehebungsthemen identifiziert wurden. Umgekehrt können Sie mit einem Problembehebungsproblem umgehen und dessen Schweregrad verringern, indem Sie sich mit nur einem Problembehebungsthema befassen. Ihr Ansatz zur Risikominderung hängt von den Anforderungen und der Arbeitsbelastung Ihres Unternehmens ab.

Note

Die in diesem Thema enthaltenen Hinweise zur Problembehebung erfordern möglicherweise zusätzliche Informationen in anderen Ressourcen. AWS

Inhalt

- [Merkmale von Fehlkonfigurationen für Amazon ECS-Services](#)
 - [Der Amazon ECS-Service verwendet eine Aufgabendefinition, die mit erhöhten Rechten konfiguriert ist.](#)
 - [Der Amazon ECS-Service verfügt über einen Container, der eine IAM-Rolle übernehmen kann.](#)
 - [Der Amazon ECS-Service verwendet eine Aufgabendefinition, die Containern den Zugriff auf die Root-Dateisysteme ermöglicht.](#)
 - [Der Amazon ECS-Service verwendet eine Aufgabendefinition, die so konfiguriert ist, dass sie den Prozess-Namespace eines Hosts gemeinsam nutzt.](#)
 - [Der Amazon ECS-Service verwendet eine Aufgabendefinition, die mit Klartext-Anmeldeinformationen in den Umgebungsvariablen konfiguriert ist.](#)
 - [Der Amazon ECS-Service hat eine offene Sicherheitsgruppe](#)
 - [Der Amazon ECS-Service hat eine öffentliche IP-Adresse](#)
 - [Der Amazon ECS-Service verwendet eine Aufgabendefinition, die mit aktiviertem Host-Netzwerkmodus konfiguriert ist.](#)
 - [Die mit dem Amazon ECS-Service verknüpfte IAM-Rolle hat eine administrative Zugriffsrichtlinie.](#)

- [Merkmale der Sicherheitslücke für Amazon ECS-Services](#)
 - [Der Amazon ECS-Service verfügt über einen Container mit Softwareschwachstellen, die über das Netzwerk ausgenutzt werden können und deren Ausnutzung sehr wahrscheinlich ist](#)
 - [Der Amazon ECS-Service hat einen Container mit Softwareschwachstellen](#)

Merkmale von Fehlkonfigurationen für Amazon ECS-Services

Im Folgenden finden Sie Merkmale von Fehlkonfigurationen für Amazon ECS-Services und empfohlene Schritte zur Behebung.

Der Amazon ECS-Service verwendet eine Aufgabendefinition, die mit erhöhten Rechten konfiguriert ist.

Amazon ECS-Container, die mit erhöhten Rechten ausgeführt werden, verfügen über ähnliche Funktionen wie das Hostsystem und ermöglichen möglicherweise den Zugriff auf Host-Ressourcen und andere Container. Diese Konfiguration erhöht das Risiko, dass ein kompromittierter Container für den Zugriff auf oder die Änderung von Ressourcen außerhalb des vorgesehenen Bereichs verwendet werden könnte, was möglicherweise zur Flucht von Containern, unberechtigtem Zugriff auf den zugrunde liegenden Host und Sicherheitsverletzungen führen kann, die sich auf andere Container auf demselben Host auswirken. Gemäß den Standardsicherheitsprinzipien AWS empfiehlt es sich, geringste Rechte zu gewähren, d. h., dass Sie nur die Berechtigungen gewähren, die für die Ausführung einer Aufgabe erforderlich sind.

Überprüfen und ändern Sie die Aufgabendefinition

Identifizieren Sie in der Exposition den ARN der Aufgabendefinition. Öffnen Sie die Aufgabendefinition in der Amazon ECS-Konsole. Suchen Sie in der Aufgabendefinition nach dem Privileged-Flag, das in den Containerdefinitionen auf true gesetzt ist. Wenn der privilegierte Modus nicht erforderlich ist, erstellen Sie eine neue Version der Aufgabendefinition ohne das Privileged-Flag. Wenn der privilegierte Modus erforderlich ist, sollten Sie erwägen, den Container so zu konfigurieren, dass er ein schreibgeschütztes Dateisystem verwendet, um unbefugte Änderungen zu verhindern.

Der Amazon ECS-Service verfügt über einen Container, der eine IAM-Rolle übernehmen kann.

Mit IAM-Rollen können Amazon ECS-Aufgaben mithilfe temporärer Anmeldeinformationen sicher auf andere AWS Services zugreifen. Rollen zur Aufgabenausführung können für Amazon ECS-Aufgaben erforderlich sein, bei denen der Container mit anderen AWS Ressourcen interagieren muss. Dies ist zwar manchmal für die Container-Funktionalität erforderlich, falsch konfigurierte

Rollen können jedoch übermäßige Rechte gewähren, die von Angreifern ausgenutzt werden können, wenn ein Container kompromittiert wird, was möglicherweise unbefugten Zugriff auf AWS Ressourcen, Datendiebstahl oder unbefugte Änderung Ihrer Infrastruktur ermöglicht. Gemäß den Standardsicherheitsprinzipien AWS empfiehlt es, den Zugriff mit den geringsten Rechten zu implementieren und die IAM-Rollen zu überprüfen, die Ihren Amazon ECS-Aufgaben zugeordnet sind.

Überprüfen Sie die angehängten Rollen

Gehen Sie zum IAM-Dashboard und wählen Sie die identifizierte Rolle aus. Überprüfen Sie die der IAM-Rolle zugeordnete Berechtigungsrichtlinie. Wenn für die Aufgabe eine Interaktion mit anderen AWS Diensten erforderlich ist, behalten Sie die Rolle „Aufgabenausführung“ bei und ziehen Sie in Betracht, Berechtigungen mit den geringsten Rechten anzuwenden. Andernfalls erstellen Sie eine neue Version der Aufgabendefinition ohne die Ausführungsrolle.

Der Amazon ECS-Service verwendet eine Aufgabendefinition, die Containern den Zugriff auf die Root-Dateisysteme ermöglicht.

Amazon ECS-Container mit Zugriff auf das Host-Root-Dateisystem können potenziell kritische Dateien auf dem Hostsystem lesen, ändern oder ausführen. Diese Konfiguration erhöht das Risiko, dass ein kompromittierter Container für den Zugriff auf oder die Änderung von Ressourcen außerhalb des vorgesehenen Bereichs verwendet werden könnte, wodurch möglicherweise sensible Daten im Host-Dateisystem offengelegt werden. Gemäß den Standardsicherheitsprinzipien AWS empfiehlt es sich, geringste Rechte zu gewähren, d. h., dass Sie nur die Berechtigungen gewähren, die für die Ausführung einer Aufgabe erforderlich sind.

Überprüfen und ändern Sie Container mit Zugriff auf das Host-Dateisystem

Identifizieren Sie im Expositionsergebnis den ARN der Aufgabendefinition. Öffnen Sie die Aufgabendefinition in der Amazon ECS-Konsole. Suchen Sie in der Aufgabendefinition nach dem Abschnitt Volumes, der Host-Pfadzuordnungen definiert. Prüfen Sie anhand der Aufgabendefinition, ob der Zugriff auf das Host-Dateisystem für die Container-Funktionalität erforderlich ist. s Falls kein Zugriff auf das Host-Dateisystem erforderlich ist, erstellen Sie eine neue Version der Aufgabendefinition und entfernen Sie alle Volume-Definitionen, die Hostpfade verwenden. Wenn Zugriff auf das Host-Dateisystem erforderlich ist, sollten Sie erwägen, den Container so zu konfigurieren, dass er ein schreibgeschütztes Dateisystem verwendet, um unbefugte Änderungen zu verhindern.

Der Amazon ECS-Service verwendet eine Aufgabendefinition, die so konfiguriert ist, dass sie den Prozess-Namespaces eines Hosts gemeinsam nutzt.

Amazon ECS-Container, die mit exponierten Namespaces ausgeführt werden, können potenziell auf Hostsystemressourcen und andere Container-Namespaces zugreifen. Diese Konfiguration könnte es einem kompromittierten Container ermöglichen, seine Isolationsgrenze zu umgehen, was dazu führen könnte, dass auf Prozesse, Netzwerkschnittstellen oder andere Ressourcen außerhalb des vorgesehenen Bereichs zugegriffen wird. Ein Prozess-ID-Namespaces (PID) sorgt für die Trennung zwischen Prozessen. Er verhindert, dass Systemprozesse sichtbar sind, und PIDs ermöglicht deren Wiederverwendung, einschließlich PID 1. Wenn der PID-Namespaces des Hosts gemeinsam mit Containern genutzt wird, könnten Container alle Prozesse auf dem Hostsystem sehen. Dies verringert den Vorteil der Isolierung auf Prozessebene zwischen dem Host und den Containern. Diese Faktoren könnten zu unberechtigtem Zugriff auf Prozesse auf dem Host selbst führen, einschließlich der Möglichkeit, diese zu manipulieren und zu beenden. Es wird AWS empfohlen, die Namespaces-Isolierung von Containern unter Einhaltung der Standardsicherheitsprinzipien aufrechtzuerhalten.

Aktualisieren Sie Aufgabendefinitionen mit offengelegten Namespaces

Öffnen Sie die Registerkarte Ressourcen der Exposure und identifizieren Sie die Aufgabendefinition mit dem exponierten Namespace. Öffnen Sie die Aufgabendefinition in der Amazon ECS-Konsole. Suchen Sie nach den PIDMode-Einstellungen mit dem Wert host, die die Prozess-ID-Namespaces mit dem Host teilen würden. Entfernen Sie die Einstellungen pidMode: host aus Ihren Aufgabendefinitionen, um sicherzustellen, dass Container mit der richtigen Namespaces-Isolierung ausgeführt werden.

Der Amazon ECS-Service verwendet eine Aufgabendefinition, die mit Klartext-Anmeldeinformationen in den Umgebungsvariablen konfiguriert ist.

Amazon ECS-Container mit Klartext-Anmeldeinformationen in Umgebungsvariablen geben vertrauliche Authentifizierungsinformationen preis, die gefährdet werden könnten, wenn ein Angreifer Zugriff auf die Aufgabendefinition, die Container-Umgebung oder die Container-Logs erhält. Dies stellt ein erhebliches Sicherheitsrisiko dar, da durchgesickerte Anmeldeinformationen für den Zugriff auf andere AWS Dienste oder Ressourcen verwendet werden könnten.

Ersetzen Sie Klartext-Anmeldeinformationen

Identifizieren Sie bei der Ermittlung der Sicherheitslücke die Aufgabendefinition durch Klartext-Anmeldeinformationen. Öffnen Sie die Aufgabendefinition in der Amazon ECS-Konsole. Suchen Sie in der Container-Definition nach Umgebungsvariablen, die sensible Werte wie AWS Zugriffsschlüssel, Datenbankkennwörter oder API-Token enthalten.

Erwägen Sie die folgenden Alternativen, um Anmeldeinformationen zu übergeben:

- Anstatt AWS Zugriffsschlüssel zu verwenden, verwenden Sie IAM-Aufgabenausführungsrollen und Aufgabenrollen, um Ihren Containern Berechtigungen zu erteilen.
- Speichern Sie Anmeldeinformationen als Geheimnisse in AWS Secrets Manager und verweisen Sie in Ihrer Aufgabendefinition darauf.

Aktualisieren der Aufgabendefinitionen

Erstellen Sie eine neue Version Ihrer Aufgabendefinition, die Anmeldeinformationen sicher verarbeitet. Aktualisieren Sie dann Ihren Amazon ECS-Service, sodass er die neue Version der Aufgabendefinition verwendet.

Der Amazon ECS-Service hat eine offene Sicherheitsgruppe

Sicherheitsgruppen dienen als virtuelle Firewalls für Ihre Amazon ECS-Aufgaben zur Steuerung des eingehenden und ausgehenden Datenverkehrs. Offene Sicherheitsgruppen, die uneingeschränkten Zugriff von jeder beliebigen IP-Adresse aus ermöglichen, können Ihre Container unberechtigtem Zugriff aussetzen und so das Risiko erhöhen, automatisierten Scan-Tools und gezielten Angriffen ausgesetzt zu werden. Es wird AWS empfohlen, den Zugriff von Sicherheitsgruppen auf bestimmte IP-Adressen und Ports gemäß den Standardsicherheitsprinzipien zu beschränken.

Überprüfen Sie die Sicherheitsgruppenregeln und bewerten Sie die aktuelle Konfiguration

Öffnen Sie die Ressource für die Amazon ECS-Sicherheitsgruppe. Prüfen Sie, welche Ports offen und über breite IP-Bereiche zugänglich sind, z. (0.0.0.0/0 or ::/0) B.

Ändern Sie die Regeln für Sicherheitsgruppen

Ändern Sie Ihre Sicherheitsgruppenregeln, um den Zugriff auf bestimmte vertrauenswürdige IP-Adressen oder Bereiche einzuschränken. Denken Sie bei der Aktualisierung Ihrer Sicherheitsgruppenregeln darüber nach, die Zugriffsanforderungen für verschiedene Netzwerksegmente zu trennen, indem Sie Regeln für jeden erforderlichen Quell-IP-Bereich erstellen oder den Zugriff auf bestimmte Ports einschränken.

Ändern Sie die Regeln für Sicherheitsgruppen

Ziehen Sie die folgenden Optionen für alternative Zugriffsmethoden in Betracht:

- Session Manager bietet sicheren Shell-Zugriff auf Ihre EC2 Amazon-Instances, ohne dass Sie eingehende Ports benötigen, SSH-Schlüssel verwalten oder Bastion-Hosts verwalten müssen.

- NACLs bieten eine zusätzliche Sicherheitsebene auf Subnetzebene. Im Gegensatz zu Sicherheitsgruppen NACLs sind sie zustandslos und erfordern, dass sowohl eingehende als auch ausgehende Regeln explizit definiert werden.

Der Amazon ECS-Service hat eine öffentliche IP-Adresse

Amazon ECS-Services mit öffentlichen IP-Adressen, die ihren Aufgaben zugewiesen sind, sind direkt über das Internet zugänglich. Dies kann zwar für Dienste erforderlich sein, die öffentlich verfügbar sein müssen, erhöht jedoch die Angriffsfläche und das Potenzial für unbefugten Zugriff.

Identifizieren Sie Dienste mit öffentlichen IP-Adressen

Identifizieren Sie in der Risikofeststellung den Amazon ECS-Service, dem öffentliche IP-Adressen für seine Aufgaben zugewiesen wurden. Suchen Sie in der Servicekonfiguration nach `ENABLED` der `assignPublicIp` Einstellung mit dem Wert von.

Aktualisieren der Aufgabendefinitionen

Erstellen Sie eine neue Version Ihrer Aufgabendefinition, die öffentliche IP-Adressen deaktiviert. Aktualisieren Sie dann Ihren Amazon ECS-Service, sodass er die neue Version der Aufgabendefinition verwendet.

Implementieren Sie Zugriffsmuster für private Netzwerke

Für Instances, auf denen Webanwendungen ausgeführt werden, sollten Sie die Verwendung eines Load Balancer (LB) in Betracht ziehen. LBs kann so konfiguriert werden, dass Ihre Instances in privaten Subnetzen ausgeführt werden können, während der LB in einem öffentlichen Subnetz läuft und den Internetverkehr abwickelt.

Der Amazon ECS-Service verwendet eine Aufgabendefinition, die mit aktiviertem Host-Netzwerkmodus konfiguriert ist.

Amazon ECS-Container, die im Host-Netzwerkmodus ausgeführt werden, teilen sich den Netzwerk-Namespace mit dem Host, was direkten Zugriff auf die Netzwerkschnittstellen, Ports und Routing-Tabellen des Hosts ermöglicht. Diese Konfiguration umgeht die durch Container bereitgestellte Netzwerkisolierung, wodurch Dienste, die auf dem Container ausgeführt werden, möglicherweise direkt externen Netzwerken zugänglich gemacht werden und es Containern ermöglicht, die Netzwerkeinstellungen des Hosts zu ändern. Es wird AWS empfohlen, die Einhaltung der Standardsicherheitsprinzipien aufrechtzuerhalten, um Container ordnungsgemäß zu isolieren.

Deaktivieren Sie den Host-Netzwerkmodus

Identifizieren Sie in der Expositionsanalyse die Aufgabendefinition mit dem Host-Netzwerkmodus. Öffnen Sie die Aufgabendefinition in der Amazon ECS-Konsole. Suchen Sie in der Aufgabendefinition nach der Einstellung `NetworkMode` mit dem Wert `host`.

Ziehen Sie die folgenden Optionen in Betracht, um den Host-Netzwerkmodus zu deaktivieren:

- Der `awsvpc` Netzwerkmodus bietet die stärkste Netzwerkisolierung, indem er jeder Aufgabe eine eigene `elastic network interface` gibt.
- Der `bridge` Netzwerkmodus bietet Isolierung und ermöglicht gleichzeitig Portzuordnungen, um dem Host bestimmte Container-Ports zugänglich zu machen.

Aktualisieren der Aufgabendefinitionen

Erstellen Sie eine neue Version Ihrer Aufgabendefinition mit der aktualisierten Netzwerkmoduskonfiguration. Aktualisieren Sie dann Ihren Amazon ECS-Service, sodass er die neue Version der Aufgabendefinition verwendet.

Die mit dem Amazon ECS-Service verknüpfte IAM-Rolle hat eine administrative Zugriffsrichtlinie.

IAM-Rollen mit administrativen Zugriffsrichtlinien, die an Amazon ECS-Aufgaben angehängt sind, bieten umfassende Berechtigungen, die über das hinausgehen, was normalerweise für den Containerbetrieb erforderlich ist. Diese Konfiguration erhöht das Risiko, dass ein kompromittierter Container für den Zugriff auf oder die Änderung von Ressourcen in Ihrer AWS gesamten Umgebung verwendet werden könnte. Gemäß den Standardsicherheitsprinzipien AWS empfiehlt es sich, den Zugriff mit den geringsten Rechten zu implementieren, indem nur die Berechtigungen gewährt werden, die für die Ausführung einer Aufgabe erforderlich sind.

Überprüfen und identifizieren Sie die Verwaltungsrichtlinien

Identifizieren Sie in der Ressourcen-ID den Namen der IAM-Rolle. Gehen Sie zum IAM-Dashboard und wählen Sie die identifizierte Rolle aus. Überprüfen Sie die der IAM-Rolle zugeordnete Berechtigungsrichtlinie. Wenn es sich bei der Richtlinie um eine AWS verwaltete Richtlinie handelt, suchen `AdministratorAccess` Sie nach. Suchen Sie andernfalls im Richtliniendokument nach Aussagen, in denen die Aussagen `"Effect": "Allow"`, `"Action": "*"` , and `"Resource": "*"` zusammengefasst sind.

Implementieren des Zugriffs mit geringsten Berechtigungen

Ersetzen Sie Verwaltungsrichtlinien durch Richtlinien, die nur die spezifischen Berechtigungen gewähren, die für das Funktionieren der Instanz erforderlich sind. Um unnötige Berechtigungen zu identifizieren, können Sie den IAM Access Analyzer verwenden, um zu verstehen, wie Sie Ihre Richtlinie auf der Grundlage des Zugriffsverlaufs ändern können. Alternativ können Sie eine neue IAM-Rolle erstellen, um zu vermeiden, dass sich dies auf andere Anwendungen auswirkt, die die vorhandene Rolle verwenden. Erstellen Sie in diesem Szenario eine neue IAM-Rolle und ordnen Sie dann die neue IAM-Rolle der Instance zu.

Überlegungen zur sicheren Konfiguration

Wenn für die Instanz Administratorberechtigungen auf Service-Ebene erforderlich sind, sollten Sie die Implementierung dieser zusätzlichen Sicherheitskontrollen in Betracht ziehen, um das Risiko zu minimieren:

- MFA fügt eine zusätzliche Sicherheitsebene hinzu, indem es eine zusätzliche Form der Authentifizierung erfordert. Dies hilft, unbefugten Zugriff zu verhindern, selbst wenn Anmeldeinformationen kompromittiert werden.
- Durch die Einrichtung von Bedingungelementen können Sie anhand von Faktoren wie Quell-IP oder MFA-Alter einschränken, wann und wie Administratorberechtigungen verwendet werden können.

Aktualisieren der Aufgabendefinitionen

Erstellen Sie eine neue Version Ihrer Aufgabendefinition, die auf die neuen oder aktualisierten IAM-Rollen verweist. Aktualisieren Sie dann Ihren Amazon ECS-Service, sodass er die neue Version der Aufgabendefinition verwendet.

Merkmale der Sicherheitslücke für Amazon ECS-Services

Im Folgenden finden Sie Merkmale der Erreichbarkeit für Amazon ECS und empfohlene Schritte zur Problembehebung.

Der Amazon ECS-Service verfügt über einen Container mit Softwareschwachstellen, die über das Netzwerk ausgenutzt werden können und deren Ausnutzung sehr wahrscheinlich ist

1. Verstehen Sie das Risiko

Package von Ergebnissen zu Sicherheitslücken in Paketen werden Softwarepakete in Ihrer AWS Umgebung identifiziert, die häufig auftretenden Sicherheitslücken (CVEs) ausgesetzt sind.

Angreifer können diese ungepatchten Sicherheitslücken ausnutzen, um die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten zu gefährden oder auf andere Systeme zuzugreifen. ECR-Container-Images können Erkenntnisse zu Sicherheitslücken in Paketen enthalten.

2. Korrigieren Sie das Risiko

a. Paketversion aktualisieren

Überprüfen Sie die Sicherheitslücke im Paket für Ihre Lambda-Funktion. Aktualisieren Sie die Paketversion wie von Amazon Inspector vorgeschlagen. Weitere Informationen finden Sie unter [Anzeigen von Details zu Ihren Amazon Inspector Inspector-Ergebnissen](#) im Amazon Inspector Inspector-Benutzerhandbuch. Im Abschnitt Behebung der Suchdetails in der Amazon Inspector Inspector-Konsole erfahren Sie, welche Befehle Sie ausführen können, um das Paket zu aktualisieren.

b. Aktualisieren Sie die Basis-Container-Images

Erstellen und aktualisieren Sie die Basis-Container-Images regelmäßig, um Ihre Container auf dem neuesten Stand zu halten. Fügen Sie beim Neuaufbau des Images keine unnötigen Komponenten hinzu, um die Angriffsfläche zu reduzieren. Anweisungen zur Neuerstellung eines Container-Images finden [Sie unter Häufig Ihre Images neu erstellen](#).

Der Amazon ECS-Service hat einen Container mit Softwareschwachstellen

Softwarepakete, die auf Amazon ECS-Containern installiert sind, können Common Vulnerabilities and Exposures (CVEs) ausgesetzt sein. Sicherheitslücken mit niedriger Priorität sind Sicherheitslücken mit geringerem Schweregrad oder geringerer Ausnutzbarkeit als Sicherheitslücken mit hoher Priorität. Diese Sicherheitslücken stellen zwar ein geringeres unmittelbares Risiko dar, aber Angreifer können diese ungepatchten Sicherheitslücken dennoch ausnutzen, um die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten zu gefährden oder auf andere Systeme zuzugreifen.

Aktualisieren Sie die betroffenen Container-Images

Sehen Sie sich den Abschnitt Referenzen auf der Registerkarte Sicherheitslücke des Merkmals an. Die Herstellerdokumentation kann spezifische Anleitungen zur Problembehebung enthalten.

Wenden Sie die entsprechenden Abhilfemaßnahmen an, indem Sie die folgenden allgemeinen Richtlinien befolgen:

- Aktualisieren Sie Ihre Container-Images, um gepatchte Versionen der betroffenen Pakete zu verwenden.

- Aktualisieren Sie die betroffenen Abhängigkeiten in Ihrer Anwendung auf die neuesten sicheren Versionen.

Nachdem Sie Ihr Container-Image aktualisiert haben, übertragen Sie es in Ihre Container-Registry und aktualisieren Sie Ihre Amazon ECS-Aufgabendefinition, um das neue Image zu verwenden.

Zukünftige Überlegungen

Um den Sicherheitsstatus Ihrer Container-Images weiter zu verbessern, sollten Sie die Best Practices für Aufgaben und Containersicherheit von Amazon ECS befolgen. Amazon Inspector kann so konfiguriert werden, dass es automatisch CVEs nach Ihren Containern sucht. Amazon Inspector kann für automatische Problembehebungen auch in Security Hub integriert werden. Erwägen Sie die Implementierung eines regelmäßigen Patch-Zeitplans mithilfe von Systems Manager Maintenance Windows, um Unterbrechungen Ihrer Container so gering wie möglich zu halten.

Behebung von Risiken für Amazon EKS-Cluster

AWS Security Hub kann Risikopergebnisse für Amazon Elastic Kubernetes Service (Amazon EKS) - Cluster generieren.

Der Amazon EKS-Cluster, der an einer Risikofeststellung beteiligt war, und seine identifizierenden Informationen sind im Abschnitt Ressourcen der Ergebnisdetails aufgeführt. Sie können diese Ressourcendetails auf der Security Hub Hub-Konsole oder programmgesteuert mithilfe der [GetFindingsV2](#) Security Hub Hub-API abrufen.

Nachdem Sie die Ressource identifiziert haben, die an einer Risikofeststellung beteiligt war, können Sie die Ressource löschen, wenn Sie sie nicht benötigen. Durch das Löschen einer nicht benötigten Ressource können Sie Ihr Expositionsprofil und Ihre AWS Kosten reduzieren. Wenn es sich bei der Ressource um eine wichtige Ressource handelt, befolgen Sie diese empfohlenen Abhilfemaßnahmen, um das Risiko zu minimieren. Die Themen zur Problembehebung sind nach der Art des Merkmals unterteilt.

Ein einziger Risikobefund umfasst Probleme, die in mehreren Problembehebungsthemen identifiziert wurden. Umgekehrt können Sie mit einem Problembehebungsproblem umgehen und dessen Schweregrad verringern, indem Sie sich mit nur einem Problembehebungsthema befassen. Ihr Ansatz zur Risikominderung hängt von den Anforderungen und der Arbeitsbelastung Ihres Unternehmens ab.

 Note

Die in diesem Thema enthaltenen Hinweise zur Problembehebung erfordern möglicherweise zusätzliche Informationen in anderen Ressourcen. AWS

Inhalt

- [Fehlkonfigurationsmerkmale für Amazon EKS-Cluster](#)
 - [Der Amazon EKS-Cluster ermöglicht öffentlichen Zugriff](#)
 - [Der Amazon EKS-Cluster verwendet eine nicht unterstützte Kubernetes-Version](#)
 - [Der Amazon EKS-Cluster verwendet unverschlüsselte Kubernetes-Geheimnisse](#)
- [Sicherheitsanfälligkeitsmerkmale für Amazon EKS-Cluster](#)
 - [Der Amazon EKS-Cluster verfügt über einen Container mit Softwareschwachstellen, die im Netzwerk ausgenutzt werden können und deren Ausnutzung sehr wahrscheinlich ist](#)
 - [Der Amazon EKS-Cluster hat einen Container mit Softwareschwachstellen](#)

Fehlkonfigurationsmerkmale für Amazon EKS-Cluster

Im Folgenden finden Sie Merkmale von Fehlkonfigurationen für Amazon EKS-Cluster und empfohlene Schritte zur Behebung.

Der Amazon EKS-Cluster ermöglicht öffentlichen Zugriff

Der Amazon EKS-Cluster-Endpoint ist der Endpoint, den Sie für die Kommunikation mit dem Kubernetes-API-Server Ihres Clusters verwenden. Standardmäßig ist dieser Endpoint im Internet öffentlich zugänglich. Öffentliche Endpunkte erhöhen Ihre Angriffsfläche und erhöhen das Risiko eines unbefugten Zugriffs auf Ihren Kubernetes-API-Server, sodass Angreifer möglicherweise auf Cluster-Ressourcen zugreifen oder diese ändern oder auf sensible Daten zugreifen können. Gemäß den bewährten Sicherheitsmethoden AWS empfiehlt es sich, den Zugriff auf Ihren EKS-Cluster-Endpoint auf die erforderlichen IP-Bereiche zu beschränken.

Ändern Sie den Endpunktzugriff

Öffnen Sie im Expositionsnachweis die Ressource. Dadurch wird der betroffene Amazon EKS-Cluster geöffnet. Sie können Ihren Cluster so konfigurieren, dass er privaten Zugriff, öffentlichen Zugriff oder beides verwendet. Bei privatem Zugriff verwenden Kubernetes-API-Anfragen, die ihren Ursprung in der VPC Ihres Clusters haben, den privaten VPC-Endpoint. Beim öffentlichen Zugriff verwenden

Kubernetes-API-Anfragen, die von außerhalb der VPC Ihres Clusters stammen, den öffentlichen Endpunkt.

Ändern oder entfernen Sie den öffentlichen Zugriff auf den Cluster

Informationen zum Ändern des Endpunktzugriffs für einen vorhandenen Cluster finden Sie unter [Ändern des Cluster-Endpunktzugriffs](#) im Amazon Elastic Kubernetes Service Service-Benutzerhandbuch. Implementieren Sie restriktivere Regeln, die auf bestimmten IP-Bereichen oder Sicherheitsgruppen basieren. Wenn ein eingeschränkter öffentlicher Zugriff erforderlich ist, beschränken Sie den Zugriff auf bestimmte CIDR-Blockbereiche oder verwenden Sie Präfixlisten.

Der Amazon EKS-Cluster verwendet eine nicht unterstützte Kubernetes-Version

Amazon EKS unterstützt jede Kubernetes-Version für einen begrenzten Zeitraum. Das Ausführen von Clustern mit nicht unterstützten Kubernetes-Versionen kann Ihre Umgebung Sicherheitslücken aussetzen, da CVE-Patches nicht mehr für veraltete Versionen veröffentlicht werden. Nicht unterstützte Versionen können bekannte Sicherheitslücken enthalten, die von Angreifern ausgenutzt werden können, und es fehlen Sicherheitsfunktionen, die möglicherweise in neueren Versionen verfügbar sind. Es wird AWS empfohlen, Ihre Kubernetes-Version stets auf dem neuesten Stand zu halten.

Aktualisieren Sie die Kubernetes-Version

Öffnen Sie im Exposure Finding die Ressource. Dadurch wird der betroffene Amazon EKS-Cluster geöffnet. Bevor Sie Ihren Cluster aktualisieren, finden Sie [unter Verfügbare Versionen mit Standardunterstützung](#) im Amazon Elastic Kubernetes Service User Guide eine Liste der aktuell unterstützten Kubernetes-Versionen.

Der Amazon EKS-Cluster verwendet unverschlüsselte Kubernetes-Geheimnisse

Kubernetes-Geheimnisse werden standardmäßig unverschlüsselt im dem API-Server zugrunde liegenden Datenspeicher (etcd) gespeichert. Jeder mit API-Zugriff oder Zugriff auf etcd kann ein Geheimnis abrufen oder ändern. Um dies zu verhindern, sollten Sie Kubernetes-Geheimnisse im Ruhezustand verschlüsseln. Wenn Kubernetes Secrets unverschlüsselt sind, sind sie anfällig für unbefugten Zugriff, falls etcd kompromittiert wird. Da Secrets häufig sensible Informationen wie Passwörter und API-Token enthalten, kann ihre Offenlegung zu unberechtigt Zugriff auf andere Anwendungen und Daten führen. Es wird AWS empfohlen, alle vertraulichen Informationen, die in Kubernetes-Geheimnissen gespeichert sind, zu verschlüsseln.

Verschlüsseln Sie Kubernetes-Geheimnisse

Amazon EKS unterstützt die Verschlüsselung von Kubernetes-Geheimnissen mithilfe von KMS-Schlüsseln durch Envelope-Verschlüsselung. Informationen zum Aktivieren der Verschlüsselung von Kubernetes-Geheimnissen für Ihren EKS-Cluster finden Sie unter [Verschlüsseln von Kubernetes-Geheimnissen mit KMS auf vorhandenen Clustern](#) im Amazon EKS-Benutzerhandbuch.

Sicherheitsanfälligkeitsmerkmale für Amazon EKS-Cluster

Hier sind die Schwachstellenmerkmale für Amazon EKS-Cluster.

Der Amazon EKS-Cluster verfügt über einen Container mit Softwareschwachstellen, die im Netzwerk ausgenutzt werden können und deren Ausnutzung sehr wahrscheinlich ist

Softwarepakete, die auf EKS-Clustern installiert sind, können häufig auftretenden Sicherheitslücken () ausgesetzt sein. CVEs Kritische CVEs Geräte stellen erhebliche Sicherheitsrisiken für Ihre AWS Umgebung dar. Unbefugte Benutzer können diese ungepatchten Sicherheitslücken ausnutzen, um die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten zu gefährden oder auf andere Systeme zuzugreifen. Kritische Sicherheitslücken mit hoher Wahrscheinlichkeit stellen unmittelbare Sicherheitsbedrohungen dar, da Exploit-Code möglicherweise bereits öffentlich verfügbar ist und von Angreifern oder automatisierten Scan-Tools aktiv genutzt wird. Befolgt bewährte Sicherheitsmethoden und AWS empfiehlt, diese Sicherheitslücken zu patchen, um Ihre Instance vor Angriffen zu schützen.

Aktualisieren Sie die betroffenen Instanzen

Aktualisieren Sie Ihre Container-Images auf neuere Versionen, die Sicherheitsupdates für die identifizierten Sicherheitslücken enthalten. Dies beinhaltet in der Regel die Neuerstellung Ihrer Container-Images mit aktualisierten Basis-Images oder Abhängigkeiten und die anschließende Bereitstellung der neuen Images in Ihrem Amazon EKS-Cluster.

Der Amazon EKS-Cluster hat einen Container mit Softwareschwachstellen

Softwarepakete, die auf Amazon EKS-Clustern installiert sind, können Common Vulnerabilities and Exposures (CVEs) ausgesetzt sein. Bei nicht kritischen Sicherheitslücken CVEs handelt es sich um Sicherheitslücken mit geringerem Schweregrad oder geringerer Ausnutzbarkeit als kritische. CVEs Diese Sicherheitslücken stellen zwar ein geringeres unmittelbares Risiko dar, aber Angreifer können diese ungepatchten Sicherheitslücken dennoch ausnutzen, um die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten zu gefährden oder auf andere Systeme zuzugreifen. Befolgt bewährte Sicherheitsmethoden und AWS empfiehlt, diese Sicherheitslücken zu patchen, um Ihre Instance vor Angriffen zu schützen.

Aktualisieren Sie die betroffenen Instanzen

Aktualisieren Sie Ihre Container-Images auf neuere Versionen, die Sicherheitsupdates für die identifizierten Sicherheitslücken enthalten. Dies beinhaltet in der Regel die Neuerstellung Ihrer Container-Images mit aktualisierten Basis-Images oder Abhängigkeiten und die anschließende Bereitstellung der neuen Images in Ihrem Amazon EKS-Cluster.

Behebung von Risiken für IAM-Benutzer

AWS Security Hub kann Ergebnisse zur Gefährdung von AWS Identity and Access Management (IAM) -Benutzern generieren.

Auf der Security Hub Hub-Konsole werden der IAM-Benutzer, der an einer Risikofeststellung beteiligt war, und seine identifizierenden Informationen im Abschnitt Ressourcen der Ergebnisdetails aufgeführt. Programmgesteuert können Sie Ressourcendetails mithilfe der [GetFindingsV2](#) Security Hub Hub-API abrufen.

Nachdem Sie die Ressource identifiziert haben, die an einer Risikofeststellung beteiligt war, können Sie die Ressource löschen, falls Sie sie nicht benötigen. Durch das Löschen einer nicht benötigten Ressource können Sie Ihr Expositionsprofil und Ihre AWS Kosten reduzieren. Wenn es sich bei der Ressource um eine wichtige Ressource handelt, befolgen Sie diese empfohlenen Abhilfemaßnahmen, um das Risiko zu minimieren. Die Themen zur Problembehebung sind nach der Art des Merkmals unterteilt.

Ein einzelnes Problembehebungsergebnis umfasst Probleme, die in mehreren Problembehebungsthemen identifiziert wurden. Umgekehrt können Sie mit einem Problembehebungsproblem umgehen und dessen Schweregrad verringern, indem Sie sich mit nur einem Problembehebungsthema befassen. Ihr Ansatz zur Risikominderung hängt von den Anforderungen und der Arbeitsbelastung Ihres Unternehmens ab.

Note

Die in diesem Thema enthaltenen Hinweise zur Problembehebung erfordern möglicherweise zusätzliche Informationen in anderen Ressourcen. AWS

Bewährte IAM-Methoden empfehlen, IAM-Rollen zu erstellen oder einen Verbund mit einem Identitätsanbieter für den Zugriff mit temporären Anmeldeinformationen zu AWS verwenden, anstatt einzelne IAM-Benutzer zu erstellen. Wenn dies für Ihre Organisation und Ihren Anwendungsfall eine Option ist, empfehlen wir, statt IAM-Benutzer zu verwenden, zu Rollen oder einem Verbund zu wechseln. Weitere Informationen finden Sie unter [IAM-Benutzer](#) im IAM-Benutzerhandbuch.

Inhalt

- [Merkmale von Fehlkonfigurationen für IAM-Benutzer](#)
 - [Der IAM-Benutzer hat eine Richtlinie mit Administratorzugriff](#)
 - [Der IAM-Benutzer hat MFA nicht aktiviert](#)
 - [Der IAM-Benutzer hat eine Richtlinie mit Administratorzugriff auf ein AWS-Service](#)
 - [Das AWS Konto für den IAM-Benutzer hat schwache Passwortrichtlinien](#)
 - [Der IAM-Benutzer hat unbenutzte Anmeldeinformationen](#)
 - [Der IAM-Benutzer hat ungerichtete Zugriffsschlüssel](#)
 - [Der IAM-Benutzer verfügt über eine Richtlinie, die uneingeschränkten Zugriff auf die Entschlüsselung von KMS-Schlüsseln ermöglicht](#)

Merkmale von Fehlkonfigurationen für IAM-Benutzer

Im Folgenden finden Sie Merkmale von Fehlkonfigurationen für IAM-Benutzer und empfohlene Schritte zur Behebung.

Der IAM-Benutzer hat eine Richtlinie mit Administratorzugriff

IAM-Richtlinien gewähren IAM-Benutzern eine Reihe von Rechten beim Zugriff auf Ressourcen. Verwaltungsrichtlinien gewähren IAM-Benutzern umfassende Berechtigungen für AWS Dienste und Ressourcen. Die Bereitstellung vollständiger Administratorrechte anstelle der Mindestberechtigungen, die der Benutzer benötigt, kann das Ausmaß eines Angriffs erhöhen, wenn Anmeldeinformationen kompromittiert werden. Gemäß den Standardsicherheitsprinzipien AWS empfiehlt es sich, die geringsten Rechte zu gewähren, d. h., dass Sie nur die für die Ausführung einer Aufgabe erforderlichen Berechtigungen gewähren.

1. Überprüfen und identifizieren Sie die Verwaltungsrichtlinien — Geben Sie in der Ressourcen-ID den Namen der IAM-Rolle an. Gehen Sie zum IAM-Dashboard und wählen Sie die identifizierte Rolle aus. Überprüfen Sie die dem IAM-Benutzer zugeordnete Berechtigungsrichtlinie. Wenn es sich bei der Richtlinie um eine AWS verwaltete Richtlinie handelt, suchen Sie nach `AdministratorAccess` oder `IAMFullAccess`. Andernfalls suchen Sie im Richtliniendokument nach Aussagen, in denen die Aussagen `"Effect": "Allow"` mit `"Action": "*" über stehen"Resource": "*".`
2. Implementieren Sie den geringsten Zugriff — Ersetzen Sie die Verwaltungsrichtlinien für Dienste durch solche, die nur die spezifischen Berechtigungen gewähren, die der Benutzer benötigt, um zu funktionieren. Weitere Informationen zu bewährten Sicherheitsmethoden für IAM-Richtlinien finden

Sie im Benutzerhandbuch unter [Anwenden von Berechtigungen mit](#) den geringsten Rechten.AWS Identity and Access Management Um unnötige Berechtigungen zu identifizieren, können Sie den IAM Access Analyzer verwenden, um zu verstehen, wie Sie Ihre Richtlinie auf der Grundlage des Zugriffsverlaufs ändern können. Weitere Informationen finden Sie im AWS Identity and Access Management Benutzerhandbuch unter [Ergebnisse für externen und ungenutzten Zugriff](#).

3. Überlegungen zur sicheren Konfiguration — Wenn Dienstadministratorrechte für die Instanz erforderlich sind, sollten Sie die Implementierung dieser zusätzlichen Sicherheitskontrollen in Betracht ziehen, um das Risiko zu minimieren:
 - Multi-Faktor-Authentifizierung (MFA) — MFA fügt eine zusätzliche Sicherheitsebene hinzu, da eine zusätzliche Form der Authentifizierung erforderlich ist. Dies hilft, unbefugten Zugriff zu verhindern, selbst wenn Anmeldeinformationen kompromittiert werden. Weitere Informationen finden Sie im AWS Identity and Access Management Benutzerhandbuch unter [Multi-Faktor-Authentifizierung \(MFA\) erforderlich](#).
 - IAM-Bedingungen — Durch die Einrichtung von Bedingungelementen können Sie anhand von Faktoren wie Quell-IP oder MFA-Alter einschränken, wann und wie Administratorberechtigungen verwendet werden können. Weitere Informationen finden Sie im Benutzerhandbuch unter [Verwenden von Bedingungen in IAM-Richtlinien](#), um den Zugriff weiter einzuschränken.AWS Identity and Access Management
 - Berechtigungsgrenzen — Berechtigungsgrenzen legen die maximale Anzahl von Berechtigungen fest, die eine Rolle haben kann, und bieten so Richtlinien für Rollen mit Administratorzugriff. Weitere Informationen finden Sie im Benutzerhandbuch unter [Verwenden von Berechtigungsgrenzen, um die Rechteverwaltung innerhalb eines Kontos zu delegieren](#).AWS Identity and Access Management

Der IAM-Benutzer hat MFA nicht aktiviert

Multi-Factor Authentication (MFA) bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Wenn MFA aktiviert ist und sich ein IAM-Benutzer auf einer AWS Website anmeldet, wird er aufgefordert, seinen Benutzernamen, sein Passwort und einen Authentifizierungscode von seinem AWS MFA-Gerät einzugeben. Der authentifizierende Prinzipal muss über ein Gerät verfügen, das einen zeitkritischen Schlüssel ausgibt und Kenntnisse über Anmeldeinformationen haben muss. Ohne MFA erhält ein Angreifer vollen Zugriff auf die Benutzerberechtigungen, wenn das Passwort eines Benutzers AWS kompromittiert wird. Gemäß den Standardsicherheitsprinzipien wird AWS empfohlen, MFA für alle Konten und Benutzer zu aktivieren, die AWS Management Console Zugriff haben.

Überprüfen Sie die MFA-Typen

AWS unterstützt die folgenden [MFA-Typen](#):

- Passkeys und Sicherheitsschlüssel
- Anwendungen für virtuelle Authentifikatoren
- Hardware-TOTP-Token

Obwohl die Authentifizierung mit einem physischen Gerät in der Regel einen strengeren Sicherheitsschutz bietet, ist die Verwendung einer beliebigen Art von MFA sicherer als die Deaktivierung von MFA.

MFA aktivieren

Informationen zur Aktivierung des MFA-Typs, der Ihren Anforderungen entspricht, finden Sie unter [AWS Multi-Faktor-Authentifizierung in IAM im IAM-Benutzerhandbuch](#). Folgen Sie den Schritten für den spezifischen MFA-Typ, den Sie implementieren möchten. Für Organisationen, die viele Benutzer verwalten, möchten Sie möglicherweise die Verwendung von MFA erzwingen, indem Sie verlangen, dass MFA auf sensible Ressourcen zugreift.

Der IAM-Benutzer hat eine Richtlinie mit Administratorzugriff auf ein AWS-Service

Die Richtlinien für Dienstadministratoren gewähren IAM-Benutzern die Berechtigung, alle Aktionen innerhalb eines bestimmten AWS Dienstes auszuführen. Diese Richtlinien beinhalten in der Regel Berechtigungen, die Benutzer nicht benötigen, um ihre Aufgaben auszuführen. Wenn einem IAM-Benutzer Dienstadministratorrechte anstelle der erforderlichen Mindestberechtigungen zur Verfügung gestellt werden, erhöht sich das Ausmaß eines Angriffs, wenn Anmeldeinformationen kompromittiert werden. Gemäß den Standardsicherheitsprinzipien wird AWS empfohlen, die geringsten Rechte zu gewähren, d. h., dass Sie nur die Berechtigungen gewähren, die für die Ausführung einer Aufgabe erforderlich sind.

Überprüfen und identifizieren Sie die Richtlinien für Dienstadministratoren

Identifizieren Sie in der Ressourcen-ID den Namen der IAM-Rolle. Gehen Sie zum IAM-Dashboard und wählen Sie die identifizierte Rolle aus. Überprüfen Sie die dem IAM-Benutzer zugeordnete Berechtigungsrichtlinie. Wenn es sich bei der Richtlinie um eine von AWS verwaltete Richtlinie handelt, suchen Sie nach `AdministratorAccess` oder `IAMFullAccess`. Andernfalls suchen Sie im Richtliniendokument nach Aussagen, die die Aussagen `"enthaltenEffect": "Allow"` mit `"Action": "*" over "Resource": "*"`.

Implementieren des Zugriffs mit geringsten Berechtigungen

Ersetzen Sie die Verwaltungsrichtlinien für Dienste durch solche, die nur die spezifischen Berechtigungen gewähren, die für die Funktion des Benutzers erforderlich sind. Um unnötige Berechtigungen zu identifizieren, können Sie den IAM Access Analyzer verwenden, um zu verstehen, wie Sie Ihre Richtlinie auf der Grundlage des Zugriffsverlaufs ändern können.

Überlegungen zur sicheren Konfiguration

Wenn für die Instanz Administratorberechtigungen des Dienstes erforderlich sind, sollten Sie die Implementierung dieser zusätzlichen Sicherheitskontrollen in Betracht ziehen, um das Risiko zu verringern:

- MFA fügt eine zusätzliche Sicherheitsebene hinzu, indem es eine zusätzliche Form der Authentifizierung erfordert. Dies hilft, unbefugten Zugriff zu verhindern, selbst wenn Anmeldeinformationen kompromittiert werden.
- Verwenden Sie Bedingungelemente, um anhand von Faktoren wie Quell-IP oder MFA-Alter einzuschränken, wann und wie Administratorberechtigungen verwendet werden können.
- Verwenden Sie Berechtigungsgrenzen, um die maximale Anzahl an Berechtigungen festzulegen, die eine Rolle haben kann, und geben Sie so Richtlinien für Rollen mit Administratorzugriff.

Das AWS Konto für den IAM-Benutzer hat schwache Passwortrichtlinien

Passwortrichtlinien schützen vor unbefugtem Zugriff, indem sie Mindestanforderungen an die Komplexität von IAM-Benutzerkennwörtern durchsetzen. Ohne strenge Passwortrichtlinien besteht ein erhöhtes Risiko, dass Benutzerkonten durch das Erraten von Passwörtern oder Brute-Force-Angriffe gefährdet werden. Gemäß den üblichen Sicherheitsprinzipien AWS empfiehlt es, eine sichere Passwortrichtlinie zu implementieren, um sicherzustellen, dass Benutzer komplexe Passwörter erstellen, die schwer zu erraten sind.

Konfigurieren Sie eine sichere Passwortrichtlinie

Gehen Sie zum IAM-Dashboard und navigieren Sie zu den Kontoeinstellungen. Prüfen Sie die aktuellen Passwortrichtlinien für Ihr Konto, einschließlich der Mindestlänge, der erforderlichen Zeichentypen und der Einstellungen für das Ablaufen von Passwörtern.

Es wird AWS empfohlen, bei der Festlegung Ihrer Passwortrichtlinie mindestens die folgenden bewährten Methoden zu befolgen:

- Erfordert mindestens einen Großbuchstaben.

- Erfordert mindestens einen Kleinbuchstaben.
- Erfordert mindestens ein Symbol.
- Erfordert mindestens eine Zahl.
- Erfordert mindestens acht Zeichen.

Zusätzliche Sicherheitsüberlegungen

Ziehen Sie zusätzlich zu einer strengen Passwortrichtlinie die folgenden zusätzlichen Sicherheitsmaßnahmen in Betracht:

- MFA fügt eine zusätzliche Sicherheitsebene hinzu, indem es eine zusätzliche Form der Authentifizierung erfordert. Dies hilft, unbefugten Zugriff zu verhindern, selbst wenn Anmeldeinformationen kompromittiert werden.
- Einrichtung von Bedingungelementen, um einzuschränken, wann und wie Administratorberechtigungen verwendet werden können, basierend auf Faktoren wie Quell-IP oder MFA-Alter.

Der IAM-Benutzer hat unbenutzte Anmeldeinformationen

Unbenutzte Anmeldeinformationen, einschließlich Kennwörter und Zugriffsschlüssel, die 90 Tage oder länger inaktiv geblieben sind, stellen ein Sicherheitsrisiko für Ihre AWS Umgebung dar. Diese ungenutzten Anmeldeinformationen stellen potenzielle Angriffsvektoren für Angreifer dar und vergrößern die Gesamtangriffsfläche Ihres Unternehmens. Um Ihre Angriffsfläche zu verringern, AWS empfiehlt es sich, Anmeldedaten zu deaktivieren oder zu entfernen, die seit 90 Tagen oder länger nicht verwendet wurden.

Deaktivieren oder entfernen Sie ungenutzte Anmeldeinformationen

Öffnen Sie im Expositionsnachweis die Ressource. Dadurch wird das Fenster mit den Benutzerdetails geöffnet. Bevor Sie Maßnahmen in Bezug auf ungenutzte Anmeldeinformationen ergreifen, sollten Sie die möglichen Auswirkungen auf Ihre Umgebung abschätzen. Das Entfernen von Anmeldeinformationen ohne angemessene Prüfung kann zu Störungen bei Hintergrundprozessen, geplanten Aufträgen und mehr führen. Ziehen Sie vor dem endgültigen Löschen eine kurze Deaktivierungszeit in Betracht, um zu überprüfen, welche Auswirkungen das Entfernen der ungenutzten Anmeldeinformationen hat.

Ergreifen Sie je nach Anmeldeinformationstyp die entsprechende Maßnahme:

- Bei unbenutzten Konsolenkennwörtern sollten Sie zunächst das Passwort ändern und es vorübergehend deaktivieren. Wenn keine Probleme auftreten, fahren Sie mit der dauerhaften Deaktivierung oder Löschung fort.
- Bei ungenutzten Zugangsschlüsseln sollten Sie zunächst die Deaktivierung des Schlüssels in Betracht ziehen. Nachdem Sie bestätigt haben, dass keine Systeme betroffen sind, fahren Sie mit der dauerhaften Deaktivierung oder Löschung fort.
- Bei ungenutzten Benutzern sollten Sie erwägen, den Benutzer vorübergehend zu deaktivieren, indem Sie eine restriktive Richtlinie anhängen, bevor Sie ihn vollständig löschen.

Der IAM-Benutzer hat ungerichtete Zugriffsschlüssel

Zugriffsschlüssel bestehen aus einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel, die den programmatischen Zugriff auf Ressourcen ermöglichen. AWS Wenn Zugriffsschlüssel über einen längeren Zeitraum unverändert bleiben, erhöhen sie das Risiko eines unbefugten Zugriffs, wenn sie kompromittiert werden. Gemäß den bewährten Sicherheitsmethoden AWS empfiehlt es sich, die Zugangsschlüssel alle 90 Tage zu wechseln, um das Zeitfenster zu minimieren, in dem Angreifer kompromittierte Anmeldeinformationen verwenden können.

Zugriffstasten rotieren

Öffnen Sie im Expositionsnachweis die Ressource. Dadurch wird das Fenster mit den Benutzerdetails geöffnet. Informationen zur Rotation von Zugriffsschlüsseln finden Sie unter [Zugriffsschlüssel für IAM-Benutzer verwalten](#) im IAM-Benutzerhandbuch.

Der IAM-Benutzer verfügt über eine Richtlinie, die uneingeschränkten Zugriff auf die Entschlüsselung von KMS-Schlüsseln ermöglicht

AWS KMS ermöglicht es Ihnen, kryptografische Schlüssel zu erstellen und zu verwalten, die zum Schutz Ihrer Daten verwendet werden. IAM-Richtlinien, die uneingeschränkte AWS KMS Entschlüsselungsberechtigungen (z. B. `kms:Decrypt` oder `kms:ReEncryptFrom`) für alle KMS-Schlüssel zulassen, können zu unberechtigtem Datenzugriff führen, wenn die Anmeldeinformationen eines IAM-Benutzers kompromittiert werden. Wenn sich ein Angreifer Zugriff auf diese Anmeldeinformationen verschafft, könnte er möglicherweise alle verschlüsselten Daten in Ihrer Umgebung entschlüsseln, zu denen auch vertrauliche Daten gehören könnten. Gemäß den bewährten Sicherheitsmethoden AWS empfiehlt es sich, die Implementierung der geringsten Rechte zu implementieren, indem die AWS KMS Entschlüsselungsberechtigungen auf bestimmte Schlüssel beschränkt werden, die Benutzer für ihre Aufgaben benötigen.

Implementieren der geringstmöglichen Zugriffsrechte

Öffnen Sie unter Exposure Finding die Ressource. Dadurch wird das Fenster mit den IAM-Richtlinien geöffnet. Suchen Sie in KMS nach Berechtigungen, die `kms: Decrypt` oder `kms: ReEncryptFrom` oder `KMS: *` mit der Ressourcenspezifikation von zulassen. "*" Aktualisieren Sie die Richtlinie, um die AWS KMS Entschlüsselungsberechtigungen auf die jeweils benötigten Schlüssel zu beschränken. Ändern Sie die Richtlinie, um die "*" Ressource durch die spezifischen erforderlichen AWS KMS Schlüssel ARNs zu ersetzen.

Überlegungen zur sicheren Konfiguration

Erwägen Sie, Bedingungen hinzuzufügen, um weiter einzuschränken, wann diese Berechtigungen verwendet werden können. Sie können beispielsweise Entschlüsselungsvorgänge auf bestimmte VPC-Endpunkte oder Quell-IP-Bereiche beschränken. Sie können auch Schlüsselrichtlinien konfigurieren, um weiter einzuschränken, wer bestimmte KMS-Schlüssel verwenden kann.

Behebung von Risiken für Lambda-Funktionen

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

AWS Security Hub kann Ergebnisse zur Gefährdung von AWS Lambda (Lambda-) Funktionen generieren.

In der Security Hub Hub-Konsole sind die Lambda-Funktion, die an einer Risikofeststellung beteiligt war, und ihre identifizierenden Informationen im Abschnitt Ressourcen der Ergebnisdetails aufgeführt. Programmgesteuert können Sie Ressourcendetails mithilfe der [GetFindingsV2](#) Security Hub Hub-API abrufen.

Nachdem Sie die Ressource identifiziert haben, die an einer Risikofeststellung beteiligt war, können Sie die Ressource löschen, falls Sie sie nicht benötigen. Durch das Löschen einer nicht benötigten Ressource können Sie Ihr Expositionsprofil und Ihre AWS Kosten reduzieren. Wenn es sich bei der Ressource um eine wichtige Ressource handelt, befolgen Sie diese empfohlenen Abhilfemaßnahmen, um das Risiko zu minimieren. Die Themen zur Problembehebung sind nach der Art des Merkmals unterteilt.

Ein einziger Risikobefund umfasst Probleme, die in mehreren Problembehebungsthemen identifiziert wurden. Umgekehrt können Sie mit einem Problembehebungsproblem umgehen und dessen

Schweregrad verringern, indem Sie sich mit nur einem Problembehebungsthema befassen. Ihr Ansatz zur Risikominderung hängt von den Anforderungen und der Arbeitsbelastung Ihres Unternehmens ab.

 Note

Die in diesem Thema enthaltenen Hinweise zur Problembehebung erfordern möglicherweise zusätzliche Informationen in anderen Ressourcen. AWS

 Note

Die in diesem Thema enthaltenen Hinweise zur Problembehebung erfordern möglicherweise zusätzliche Konsultationen in anderen AWS Quellen.

Inhalt

- [Fehlkonfigurationsmerkmale für Lambda-Funktionen](#)
 - [Die Lambda-Funktion führt eine Laufzeit aus, die nicht unterstützt wird](#)
 - [Die Lambda-Funktion wird außerhalb einer Amazon VPC bereitgestellt](#)
 - [Die Lambda-Funktion kann eine IAM-Rolle übernehmen.](#)
 - [Die der Lambda-Funktion zugeordnete IAM-Rolle hat eine administrative Zugriffsrichtlinie.](#)
 - [Die der Lambda-Funktion zugeordnete IAM-Rolle hat eine Richtlinie mit Administratorzugriff auf einen Dienst. AWS](#)
- [Erreichbarkeitsmerkmale für Lambda-Funktionen](#)
 - [Die Lambda-Funktion kann öffentlich aufgerufen werden](#)
- [Schwachstellenmerkmale für Lambda-Funktionen](#)
 - [Die Lambda-Funktion weist Softwareschwachstellen auf, die über das Netzwerk ausgenutzt werden können](#)
 - [Die Lambda-Funktion weist Softwareschwachstellen auf](#)

Fehlkonfigurationsmerkmale für Lambda-Funktionen

Im Folgenden finden Sie Merkmale von Fehlkonfigurationen für Lambda-Funktionen und empfohlene Schritte zur Behebung.

Die Lambda-Funktion führt eine Laufzeit aus, die nicht unterstützt wird

Lambda ermöglicht es Entwicklern, Code auszuführen, ohne Server bereitzustellen oder zu verwalten, und zwar über Laufzeiten, die Ihren Code in einer verwalteten Umgebung ausführen. Lambda wendet automatisch Patches und Sicherheitsupdates auf verwaltete Laufzeiten und die entsprechenden Container-Basis-Images an. Wenn eine Runtime-Version nicht mehr unterstützt wird, erhält sie keine Sicherheitsupdates, Bugfixes oder technischen Support mehr. Funktionen, die auf veralteten Laufzeiten ausgeführt werden, können Sicherheitslücken aufweisen und aufgrund von Problemen wie dem Ablauf von Zertifikaten irgendwann nicht mehr funktionieren. Darüber hinaus können Laufzeiten, die nicht unterstützt werden, anfällig für neu entdeckte Sicherheitslücken sein, für die keine Patches verfügbar sind. Gemäß den bewährten Sicherheitsmethoden empfehlen wir, gepatchte, unterstützte Laufzeiten für Lambda-Funktionen zu verwenden.

Aktualisieren Sie die Laufzeit der Funktion

Öffnen Sie auf der Registerkarte Ressourcen der Exposition die Ressource mit dem Hyperlink. Dadurch wird das Lambda-Funktionsfenster geöffnet. Um Ihre Funktion auf eine unterstützte Laufzeit zu aktualisieren, konfigurieren Sie die Runtime-Management-Konfiguration. Sie können festlegen, dass Ihre Funktion automatisch auf die neueste Runtime-Version aktualisiert wird. Bevor Sie diese Option auswählen, sollten Sie jedoch prüfen, ob automatische Upgrades Auswirkungen auf Ihre laufenden Anwendungen haben könnten. Weitere Informationen finden Sie unter [Grundlegendes zur Verwaltung von Laufzeitversionsupdates durch Lambda](#).

Die Lambda-Funktion wird außerhalb einer Amazon VPC bereitgestellt

Lambda-Funktionen werden standardmäßig mit Zugriff auf das öffentliche Internet bereitgestellt. Diese Standardkonfiguration gibt Lambda-Funktionen die Möglichkeit, AWS Service-Endpunkte und externe Endpunkte zu erreichen APIs, setzt sie aber auch potenziellen Sicherheitsrisiken aus. Funktionen mit Internetzugang könnten verwendet werden, um Daten zu exfiltrieren, mit nicht autorisierten Servern zu kommunizieren oder als Einstiegspunkte für externe Akteure zu dienen, wenn sie kompromittiert werden. Amazon VPC bietet Netzwerkisolierung, indem es Ihre Lambda-Funktionen so einschränkt, dass sie nur mit Ressourcen innerhalb Ihres definierten privaten Netzwerks kommunizieren. Gemäß den Standardsicherheitsprinzipien empfehlen wir die Bereitstellung von Lambda-Funktionen innerhalb einer VPC, um die Sicherheit durch Netzwerkisolierung zu verbessern.

Funktion an VPC anhängen

Öffnen Sie im Expositionsnachweis die Ressource mit dem Hyperlink. Dadurch wird das Lambda-Funktionsfenster geöffnet. Um Ihre Lambda-Funktion zu sichern, indem Sie ihren Netzwerkzugriff

einschränken, verbinden Sie sie mit einer VPC, die über die entsprechenden Netzwerksteuerungen verfügt. Bevor Sie Ihre Funktion an eine VPC anhängen, planen Sie den eventuell benötigten AWS Dienstzugriff ein, da Funktionen in privaten Subnetzen ohne NAT-Gateways oder VPC-Endpunkte den Service nicht erreichen können. AWS APIs Informationen zum Anhängen einer Lambda-Funktion an eine Amazon VPC in Ihrem Konto finden Sie unter [Lambda-Funktionen an eine Amazon VPC anhängen](#) in Ihrem. AWS-Konto Erwägen Sie die Verwendung von VPC-Endpunkten für die Dienstkonnektivität ohne Internetzugang, wenn Ihre Funktion den Zugriff auf AWS Dienste innerhalb eines privaten Subnetzes erfordert. Konfigurieren Sie ein NAT-Gateway, wenn Sie ausgehende Internetkonnektivität von privaten Subnetzen benötigen.

Die Lambda-Funktion kann eine IAM-Rolle übernehmen.

Lambda-Funktionen verwenden IAM-Rollen, um mit AWS Diensten zu interagieren. Diese Rollen gewähren der Lambda-Funktion Berechtigungen für den Zugriff auf AWS Ressourcen während der Ausführung. Obwohl diese Rollen manchmal erforderlich sind, damit Lambda-Funktionen ihre Aufgaben erfüllen können, sollten diese Rollen dem Prinzip der geringsten Rechte folgen. Gemäß den Standardsicherheitsprinzipien AWS empfiehlt es sich, zu überprüfen, ob die mit der Rolle verknüpften Berechtigungen auf der Grundlage der beabsichtigten Funktionalität der Funktion angemessen sind.

1. Stellen Sie fest, ob die angehängte IAM-Rolle erforderlich ist

Stellen Sie fest, ob für die Lambda-Funktion eine IAM-Ausführungsrolle konfiguriert werden muss. Für den Betrieb der meisten Lambda-Funktionen sind grundlegende Berechtigungen erforderlich, z. B. das Schreiben von Protokollen in CloudWatch. Überprüfen Sie die der Ausführungsrolle der Funktion zugewiesenen Berechtigungen und stellen Sie fest, ob die IAM-Rolle für die Funktion erforderlich ist. Informationen zu Lambda-Ausführungsrollen finden Sie unter [Definieren von Lambda-Funktionsberechtigungen mit einer Ausführungsrolle](#) im AWS Lambda Entwicklerhandbuch.

2. Implementieren des Zugriffs mit geringsten Berechtigungen

Ersetzen Sie zu großzügige Richtlinien durch Richtlinien, die nur die spezifischen Berechtigungen gewähren, die für den Betrieb der Funktion erforderlich sind. Informationen zu bewährten Sicherheitsmethoden für IAM-Rollen finden Sie im Benutzerhandbuch unter [Anwenden von Berechtigungen mit den geringsten Rechten](#). AWS Identity and Access Management Um unnötige Berechtigungen zu identifizieren, können Sie den IAM Access Analyzer verwenden, um zu verstehen, wie Sie Ihre Richtlinie auf der Grundlage des Zugriffsverlaufs ändern können. Weitere Informationen finden Sie im AWS Identity and Access Management Benutzerhandbuch unter

[Ergebnisse für externen und ungenutzten Zugriff](#). Alternativ können Sie eine neue IAM-Rolle erstellen, um zu vermeiden, dass andere Lambda-Funktionen beeinträchtigt werden, die die vorhandene Rolle verwenden. Erstellen Sie in diesem Szenario eine neue IAM-Rolle und ordnen Sie dann die neue IAM-Rolle der Instanz zu. Anweisungen zum Ersetzen einer IAM-Rolle für eine Funktion finden Sie unter [Aktualisieren der Ausführungsrolle einer Funktion im AWS Lambda Entwicklerhandbuch](#).

Die der Lambda-Funktion zugeordnete IAM-Rolle hat eine administrative Zugriffsrichtlinie.

Administrative Zugriffsrichtlinien bieten Lambda-Funktionen umfassende Berechtigungen für AWS Dienste und Ressourcen. Diese Richtlinien beinhalten in der Regel Berechtigungen, die für die Funktionalität nicht erforderlich sind. Die Bereitstellung einer IAM-Identität mit einer administrativen Zugriffsrichtlinie für eine Lambda-Funktion anstelle der Mindestberechtigungen, die die Ausführungsrolle benötigt, kann den Umfang eines Angriffs erhöhen, wenn die Funktion beeinträchtigt wird. Gemäß den Standardsicherheitsprinzipien AWS empfiehlt es sich, die geringsten Rechte zu gewähren, d. h., dass Sie nur die Berechtigungen gewähren, die für die Ausführung einer Aufgabe erforderlich sind.

1. Überprüfen und identifizieren Sie die Verwaltungsrichtlinien

Identifizieren Sie in der Risikoprüfung den Rollennamen. Gehen Sie zum IAM-Dashboard und suchen Sie die Rolle mit dem zuvor identifizierten Rollennamen. Überprüfen Sie die der IAM-Rolle beigefügte Berechtigungsrichtlinie. Wenn es sich bei der Richtlinie um eine AWS verwaltete Richtlinie handelt, suchen Sie nach AdministratorAccess oder IAMFullAccess. Suchen Sie andernfalls im Strategiedokument nach Aussagen, die die Aussagen "Effect": "Allow", "Action": "*" "Resource": "*" zusammen enthalten.

2. Implementieren des Zugriffs mit geringsten Berechtigungen

Ersetzen Sie Verwaltungsrichtlinien durch solche, die nur die spezifischen Berechtigungen gewähren, die für den Betrieb der Funktion erforderlich sind. Weitere Informationen zu bewährten Sicherheitsmethoden für IAM-Rollen finden Sie im Benutzerhandbuch unter [Anwenden von Berechtigungen mit](#) den geringsten Rechten.AWS Identity and Access Management Um unnötige Berechtigungen zu identifizieren, können Sie den IAM Access Analyzer verwenden, um zu erfahren, wie Sie Ihre Richtlinie auf der Grundlage des Zugriffsverlaufs ändern können. Weitere Informationen finden Sie im AWS Identity and Access Management Benutzerhandbuch unter [Ergebnisse für externen und ungenutzten Zugriff](#). Alternativ können Sie eine neue IAM-Rolle erstellen, um zu vermeiden, dass andere Lambda-Funktionen, die die vorhandene Rolle

verwenden, beeinträchtigt werden. Erstellen Sie in diesem Szenario eine neue IAM-Rolle. Ordnen Sie dann die neue Rolle der Instanz zu. Informationen zum Ersetzen einer IAM-Rolle für eine Funktion finden Sie unter [Aktualisieren der Ausführungsrolle einer Funktion](#) im AWS Lambda Entwicklerhandbuch.

3. Überlegungen zur sicheren Konfiguration

Wenn für die Instanz Administratorzugriffsberechtigungen erforderlich sind, sollten Sie die Implementierung dieser zusätzlichen Sicherheitskontrollen in Betracht ziehen, um das Risiko zu minimieren:

- **Multi-Faktor-Authentifizierung (MFA)** — MFA fügt eine zusätzliche Sicherheitsebene hinzu, da eine zusätzliche Form der Authentifizierung erforderlich ist. Dies hilft, unbefugten Zugriff zu verhindern, selbst wenn Anmeldeinformationen kompromittiert werden. Weitere Informationen finden Sie im AWS Identity and Access Management Benutzerhandbuch unter [Multi-Faktor-Authentifizierung \(MFA\) erforderlich](#).
- **IAM-Bedingungen** — Durch die Einrichtung von Bedingungelementen können Sie anhand von Faktoren wie Quell-IP oder MFA-Alter einschränken, wann und wie Administratorberechtigungen verwendet werden können. Weitere Informationen finden Sie im [IAM-Benutzerhandbuch unter Verwenden von Bedingungen in IAM-Richtlinien, um den Zugriff weiter einzuschränken](#).
- **Berechtigungsgrenzen** — Berechtigungsgrenzen legen die maximale Anzahl von Berechtigungen fest, die eine Rolle haben kann, und bieten so Richtlinien für Rollen mit Administratorzugriff. Weitere Informationen finden Sie im Benutzerhandbuch unter [Verwenden von Berechtigungsgrenzen, um die Rechteverwaltung innerhalb eines Kontos zu delegieren](#). AWS Identity and Access Management

Die der Lambda-Funktion zugeordnete IAM-Rolle hat eine Richtlinie mit Administratorzugriff auf einen Dienst. AWS

Mithilfe von Dienstadministratorrichtlinien können Lambda-Funktionen alle Aktionen innerhalb eines bestimmten AWS Dienstes ausführen. Diese Richtlinien gewähren in der Regel mehr Berechtigungen, als für den Betrieb einer Funktion erforderlich sind. Wenn eine Lambda-Funktion mit einer Service-Admin-Richtlinie kompromittiert wird, könnte ein Angreifer diese Berechtigungen verwenden, um potenziell auf sensible Daten oder Dienste in Ihrer AWS Umgebung zuzugreifen oder diese zu ändern. Gemäß den Standardsicherheitsprinzipien empfehlen wir, die geringsten Rechte zu gewähren, was bedeutet, dass Sie nur die Berechtigungen gewähren, die für die Ausführung einer Aufgabe erforderlich sind.

1. Überprüfen und identifizieren Sie die Verwaltungsrichtlinien

Identifizieren Sie im Expositionsbericht den Rollennamen im ARN. Gehen Sie zum IAM-Dashboard und suchen Sie den Rollennamen. Überprüfen Sie die der Rolle zugeordnete Berechtigungsrichtlinie. Wenn es sich bei der Richtlinie um eine AWS verwaltete Richtlinie handelt, suchen Sie nach `AdministratorAccess` oder `IAMFullAccess`. Andernfalls suchen Sie im Richtliniendokument nach Aussagen, die die Aussagen `"Effect": "Allow"`, `"Action": "*"` und enthalten `"Resource": "*"`.

2. Implementieren des Zugriffs mit geringsten Berechtigungen

Ersetzen Sie Verwaltungsrichtlinien durch solche, die nur die spezifischen Berechtigungen gewähren, die für den Betrieb der Funktion erforderlich sind. Weitere Informationen finden Sie unter [Anwenden von geringsten Berechtigungen](#) im AWS Identity and Access Management-Benutzerhandbuch. Um unnötige Berechtigungen zu identifizieren, können Sie den IAM Access Analyzer verwenden, um zu verstehen, wie Sie Ihre Richtlinie auf der Grundlage des Zugriffsverlaufs ändern können. Weitere Informationen finden Sie im AWS Identity and Access Management Benutzerhandbuch unter [Ergebnisse für externen und ungenutzten Zugriff](#). Alternativ können Sie eine neue IAM-Rolle erstellen, um zu vermeiden, dass andere Lambda-Funktionen beeinträchtigt werden, die die vorhandene Rolle verwenden. Erstellen Sie in diesem Szenario eine neue IAM-Rolle und ordnen Sie dann die neue IAM-Rolle der Instanz zu. Anweisungen zum Ersetzen einer IAM-Rolle für eine Funktion finden Sie unter [Aktualisieren der Ausführungsrolle einer Funktion im AWS Lambda Entwicklerhandbuch](#).

3. Überlegungen zur sicheren Konfiguration

Wenn für die Instanz Administratorberechtigungen auf Service-Ebene erforderlich sind, sollten Sie die Implementierung dieser zusätzlichen Sicherheitskontrollen in Betracht ziehen, um das Risiko zu minimieren:

- **Multi-Faktor-Authentifizierung (MFA)** — MFA fügt eine zusätzliche Sicherheitsebene hinzu, da eine zusätzliche Form der Authentifizierung erforderlich ist. Dies hilft, unbefugten Zugriff zu verhindern, selbst wenn Anmeldeinformationen kompromittiert werden. Weitere Informationen finden Sie im AWS Identity and Access Management Benutzerhandbuch unter [Multi-Faktor-Authentifizierung \(MFA\) erforderlich](#).
- **IAM-Bedingungen** — Durch die Einrichtung von Bedingungelementen können Sie anhand von Faktoren wie Quell-IP oder MFA-Alter einschränken, wann und wie Administratorberechtigungen verwendet werden können. Weitere Informationen finden Sie im Benutzerhandbuch unter [Verwenden von Bedingungen in IAM-Richtlinien, um den Zugriff weiter einzuschränken](#). AWS Identity and Access Management

- **Berechtigungsgrenzen** — Berechtigungsgrenzen legen die maximale Anzahl von Berechtigungen fest, die eine Rolle haben kann, und bieten so Richtlinien für Rollen mit Administratorzugriff. Weitere Informationen finden Sie im Benutzerhandbuch unter [Verwenden von Berechtigungsgrenzen zur Delegierung der AWS Identity and Access Management Berechtigungsverwaltung](#).

Erreichbarkeitsmerkmale für Lambda-Funktionen

Im Folgenden finden Sie Merkmale der Erreichbarkeit für Lambda-Funktionen und empfohlene Schritte zur Behebung.

Die Lambda-Funktion kann öffentlich aufgerufen werden

Ressourcenbasierte Lambda-Richtlinien bestimmen, wer Ihre Funktionen aufrufen kann. Eine Funktion mit einer Ressourcenrichtlinie, die „*“ als Prinzipal (oder gar keinen Prinzipal) enthält, ermöglicht es allen authentifizierten AWS Benutzern, sie aufzurufen. Dies stellt ein erhebliches Risiko dar, insbesondere bei Funktionen, die vertrauliche Daten verarbeiten, Ressourcen ändern oder über erweiterte Berechtigungen verfügen. Unbefugte Benutzer könnten diese Konfiguration ausnutzen, um unerwünschte Operationen auszuführen, wodurch möglicherweise Daten offengelegt, Ressourcen manipuliert oder Funktionsfunktionen missbraucht werden. Gemäß den bewährten Sicherheitsmethoden empfehlen wir, den Zugriff auf Lambda-Funktionen nur auf autorisierte Prinzipale zu beschränken.

Ändern Sie die ressourcenbasierte Richtlinie der Funktion

Öffnen Sie auf der Registerkarte Ressourcen der Exposition die Ressource mit dem Hyperlink. Dadurch wird das Lambda-Funktionsfenster geöffnet. Beschränken Sie den Zugriff auf Ihre Lambda-Funktion, indem Sie in der ressourcenbasierten Richtlinie nur autorisierte AWS Konten IDs oder bestimmte IAM-Prinzipale (Benutzer, Rollen oder Dienste) angeben. Sie können ressourcenbasierte Richtlinien nur programmgesteuert ändern.

Schwachstellenmerkmale für Lambda-Funktionen

Im Folgenden finden Sie Schwachstellenmerkmale für Lambda-Funktionen und empfohlene Schritte zur Behebung.

Die Lambda-Funktion weist Softwareschwachstellen auf, die über das Netzwerk ausgenutzt werden können

Softwarepakete, die im Lambda-Funktionscode verwendet werden, können Common Vulnerabilities and Exposures (CVEs) enthalten, bei denen die Wahrscheinlichkeit hoch ist, dass sie ausgenutzt werden. Kritische CVEs Sicherheitsrisiken stellen erhebliche Sicherheitsrisiken für Ihre AWS Umgebung dar. Angreifer können diese ungepatchten Sicherheitslücken ausnutzen, um die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten zu gefährden oder auf andere Systeme zuzugreifen. Kritische Sicherheitslücken mit hoher Wahrscheinlichkeit stellen unmittelbare Sicherheitsbedrohungen dar, da Exploit-Code möglicherweise bereits öffentlich verfügbar ist und von Angreifern oder automatisierten Scan-Tools aktiv genutzt wird. Wir empfehlen, diese Sicherheitslücken zu patchen, um Ihre Funktion vor Angriffen zu schützen.

Aktualisieren Sie die betroffenen Funktionen

Suchen Sie im Abschnitt Referenzen auf der Registerkarte Sicherheitslücke nach dieser Eigenschaft. Die Herstellerdokumentation kann spezifische Anleitungen zur Problembehebung enthalten. Aktualisieren Sie die anfälligen Bibliotheken gemäß den vom Hersteller empfohlenen Verfahren auf ihre neuesten sicheren Versionen. In der Regel hängt der Korrektur-Workflow davon ab, ob Sie das Lambda-Paket bereitgestellt haben, indem Sie eine ZIP-Datei hochgeladen oder eine Lambda-Funktion mit einem Container-Image erstellt haben. Nachdem Sie die Bibliotheken aktualisiert haben, aktualisieren Sie den Lambda-Funktionscode, um die feste Version zu verwenden. Stellen Sie anschließend die aktualisierte Version bereit.

Die Lambda-Funktion weist Softwareschwachstellen auf

Lambda-Funktionen verwenden häufig Bibliotheken und Abhängigkeiten von Drittanbietern, die Sicherheitslücken mit geringerem Schweregrad oder geringerer Ausnutzbarkeit enthalten können als kritische. CVEs Auch wenn diese unkritischen Sicherheitslücken möglicherweise nicht sofort ausgenutzt werden können, stellen sie dennoch Sicherheitslücken dar, die mit anderen Sicherheitslücken verkettet werden können, um Ihre Funktion zu gefährden. Im Laufe der Zeit könnten auch neue Exploit-Techniken auftauchen, die das Risiko dieser Sicherheitslücken erhöhen. Gemäß den üblichen Sicherheitsprinzipien empfehlen wir, diese Sicherheitslücken zu patchen, um eine sichere Umgebung aufrechtzuerhalten.

Das Merkmal finden Sie im Abschnitt Referenzen auf der Registerkarte Sicherheitslücke. Die Herstellerdokumentation kann spezifische Anleitungen zur Problembehebung enthalten. Aktualisieren Sie die anfälligen Bibliotheken gemäß den vom Hersteller empfohlenen Verfahren auf ihre neuesten sicheren Versionen. In der Regel hängt der Korrektur-Workflow davon ab, ob Sie das Lambda-Paket

bereitgestellt haben, indem Sie eine ZIP-Datei hochgeladen oder eine Lambda-Funktion mit einem Container-Image erstellt haben. Nachdem Sie die Bibliotheken aktualisiert haben, aktualisieren Sie den Lambda-Funktionscode, um die feste Version zu verwenden. Stellen Sie anschließend die aktualisierte Version bereit.

Behebung von Risiken für Amazon RDS-Funktionen

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

AWS Security Hub kann Risikopergebnisse für Amazon RDS-Funktionen generieren.

In der Security Hub Hub-Konsole sind die Amazon RDS-Funktion, die an einer Risikofeststellung beteiligt war, und ihre identifizierenden Informationen im Abschnitt Ressourcen der Ergebnisdetails aufgeführt. Programmgesteuert können Sie Ressourcendetails mithilfe der [GetFindingsV2](#) Security Hub Hub-API abrufen.

Nachdem Sie die Ressource identifiziert haben, die an einer Risikofeststellung beteiligt war, können Sie die Ressource löschen, falls Sie sie nicht benötigen. Durch das Löschen einer nicht benötigten Ressource können Sie Ihr Expositionsprofil und Ihre AWS Kosten reduzieren. Wenn es sich bei der Ressource um eine wichtige Ressource handelt, befolgen Sie diese empfohlenen Abhilfemaßnahmen, um das Risiko zu minimieren. Die Themen zur Problembehebung sind nach der Art des Merkmals unterteilt.

Ein einzelnes Problembehebungsergebnis umfasst Probleme, die in mehreren Problembehebungsthemen identifiziert wurden. Umgekehrt können Sie mit einem Problembehebungsproblem umgehen und dessen Schweregrad verringern, indem Sie sich mit nur einem Problembehebungsthema befassen. Ihr Ansatz zur Risikominderung hängt von den Anforderungen und der Arbeitsbelastung Ihres Unternehmens ab.

Note

Die in diesem Thema enthaltenen Hinweise zur Problembehebung erfordern möglicherweise zusätzliche Informationen in anderen Ressourcen. AWS

Inhalt

- [Fehlkonfigurationsmerkmale für Amazon RDS-Funktionen](#)
 - [Die Amazon RDS-DB-Instance ist mit öffentlichem Zugriff konfiguriert](#)
 - [Der Amazon RDS-DB-Cluster hat einen Snapshot, der öffentlich geteilt wird](#)
 - [Die Amazon RDS-DB-Instance hat einen Snapshot, der im Ruhezustand nicht verschlüsselt ist](#)
 - [Der Amazon RDS-DB-Cluster hat einen Snapshot, der im Ruhezustand nicht verschlüsselt ist](#)
 - [Die Amazon RDS-DB-Instance hat eine offene Sicherheitsgruppe](#)
 - [Für die Amazon RDS-DB-Instance ist die IAM-Datenbankauthentifizierung deaktiviert](#)
 - [Die Amazon RDS-DB-Instance verwendet den Standard-Admin-Benutzernamen](#)
 - [Der Amazon RDS-DB-Cluster verwendet den Standard-Admin-Benutzernamen](#)
 - [Für die Amazon RDS-DB-Instance sind automatische Upgrades für kleinere Versionen deaktiviert](#)
 - [Für die Amazon RDS-DB-Instance sind automatische Backups deaktiviert](#)
 - [Für die Amazon RDS-DB-Instance ist der Löschschutz deaktiviert](#)
 - [Der Löschschutz für den Amazon RDS-DB-Cluster ist deaktiviert](#)
 - [Die Amazon RDS-DB-Instance verwendet den Standardport für die Datenbank-Engine](#)
 - [Die Amazon RDS-DB-Instance ist nicht durch einen Backup-Plan abgedeckt](#)

Fehlkonfigurationsmerkmale für Amazon RDS-Funktionen

Im Folgenden werden die Merkmale der Fehlkonfiguration und die Schritte zur Behebung von Amazon RDS-Funktionen beschrieben.

Die Amazon RDS-DB-Instance ist mit öffentlichem Zugriff konfiguriert

Amazon RDS-Instances mit öffentlichem Zugriff sind potenziell über das Internet über ihre Endpunkte zugänglich. Während für die Instance-Funktionalität manchmal ein öffentlicher Zugriff erforderlich ist, kann diese Konfiguration als potenzieller Angriffsvektor für unbefugte Benutzer verwendet werden, die versuchen, auf Ihre Datenbank zuzugreifen. Öffentlich zugängliche Datenbanken können Port-Scans, Brute-Force-Angriffen und Ausnutzungsversuchen ausgesetzt sein. Gemäß den üblichen Sicherheitsprinzipien empfehlen wir Ihnen, die öffentliche Nutzung Ihrer Datenbankressourcen zu begrenzen.

1. Ändern Sie die Einstellungen für den öffentlichen Zugriff

Öffnen Sie in der Expositionsanalyse die Ressource mit dem Hyperlink. Dadurch wird die betroffene DB-Instance geöffnet. Prüfen Sie anhand Ihrer Anwendungsarchitektur, ob die DB-Instance öffentlich zugänglich sein muss. Weitere Informationen finden Sie unter [Einrichtung eines öffentlichen oder privaten Zugriffs in Amazon RDS](#).

Der Amazon RDS-DB-Cluster hat einen Snapshot, der öffentlich geteilt wird

Auf öffentliche Snapshots kann jeder zugreifen AWS-Konto, wodurch sensible Daten möglicherweise unbefugten Benutzern zugänglich gemacht werden. Jeder AWS-Konto ist berechtigt, diese öffentlichen Snapshots zu kopieren und daraus DB-Instances zu erstellen, was zu Datenschutzverletzungen oder unberechtigt Datenzugriff führen kann. Gemäß den bewährten Sicherheitsmethoden empfehlen wir, den Zugriff auf Ihre Amazon RDS-Snapshots auf vertrauenswürdige Organisationen AWS-Konten und Organisationen zu beschränken.

1. Einen Amazon RDS-Snapshot für privaten Zugriff konfigurieren

Öffnen Sie in der Risikohinweise die Ressource über den Hyperlink. Informationen zum Ändern der Einstellungen für das Teilen von Snapshots finden Sie unter [Teilen eines Snapshots](#) im Amazon Aurora Benutzerhandbuch. Informationen darüber, wie Sie das Teilen von Snapshots beenden können, finden Sie unter [Stoppen der Snapshot-Freigabe](#) im Amazon Aurora Benutzerhandbuch. .

Die Amazon RDS-DB-Instance hat einen Snapshot, der im Ruhezustand nicht verschlüsselt ist

Unverschlüsselte Amazon RDS-DB-Instance-Snapshots können sensible Daten offenlegen, wenn unbefugter Zugriff auf die Speicherebene erfolgt. Ohne Verschlüsselung könnten Daten in Snapshots potenziell durch unbefugten Zugriff offengelegt werden. Dies birgt das Risiko von Datenverstößen und Compliance-Verstößen. Gemäß den bewährten Sicherheitsmethoden empfehlen wir, alle Datenbankressourcen und ihre Backups zu verschlüsseln, um die Vertraulichkeit der Daten zu wahren.

Öffnen Sie in der Risikoprüfung die Ressource mit dem Hyperlink. Dadurch wird der betroffene Snapshot geöffnet. Sie können einen vorhandenen unverschlüsselten Snapshot nicht direkt verschlüsseln. Erstellen Sie stattdessen eine verschlüsselte Kopie des unverschlüsselten Snapshots. Ausführliche Anweisungen finden Sie unter [Kopieren und Verschlüsseln von Amazon RDS-Ressourcen von DB-Cluster-Snapshots](#) im Amazon Aurora Benutzerhandbuch. ..

Der Amazon RDS-DB-Cluster hat einen Snapshot, der im Ruhezustand nicht verschlüsselt ist

Unverschlüsselte Amazon RDS-DB-Cluster-Snapshots können sensible Daten offenlegen, wenn unbefugter Zugriff auf die Speicherebene erfolgt. Ohne Verschlüsselung könnten Daten in Snapshots potenziell durch unbefugten Zugriff offengelegt werden. Dies birgt das Risiko von Datenverstößen und Compliance-Verstößen. Gemäß den bewährten Sicherheitsmethoden empfehlen wir, alle Datenbankressourcen und ihre Backups zu verschlüsseln, um die Vertraulichkeit der Daten zu wahren.

1. Erstellen Sie eine verschlüsselte Kopie des Snapshots

Öffnen Sie in der Risikoprüfung die Ressource mit dem Hyperlink. Dadurch wird der betroffene Snapshot geöffnet. Sie können einen vorhandenen unverschlüsselten Snapshot nicht direkt verschlüsseln. Erstellen Sie stattdessen eine verschlüsselte Kopie des unverschlüsselten Snapshots. Ausführliche Anweisungen finden Sie unter [Kopieren und Verschlüsseln von Amazon RDS-Ressourcen von DB-Cluster-Snapshots](#) im Amazon Aurora Benutzerhandbuch. ..

Die Amazon RDS-DB-Instance hat eine offene Sicherheitsgruppe

Sicherheitsgruppen dienen als virtuelle Firewalls für Ihre Amazon RDS-Instances, um den eingehenden und ausgehenden Datenverkehr zu kontrollieren. Offene Sicherheitsgruppen, die uneingeschränkten Zugriff von jeder IP-Adresse aus ermöglichen, können Ihre Datenbank-Instances unbefugtem Zugriff und potenziellen Angriffen aussetzen. Gemäß den Standardsicherheitsprinzipien empfehlen wir, den Zugriff von Sicherheitsgruppen auf bestimmte IP-Adressen und Ports zu beschränken, um das Prinzip der geringsten Rechte aufrechtzuerhalten.

Überprüfen Sie die Sicherheitsgruppenregeln und bewerten Sie die aktuelle Konfiguration

Öffnen Sie in der Sicherheitsanalyse die Ressource für die DB-Instance-Sicherheitsgruppe. Prüfen Sie, welche Ports offen und von weiten IP-Bereichen aus zugänglich sind, z. (0.0.0.0/0 or ::/0) B. Informationen zum Anzeigen von Sicherheitsgruppendetails finden Sie [DescribeSecurityGroups](#) in der Amazon Elastic Compute Cloud API-Referenz.

Ändern Sie die Regeln für Sicherheitsgruppen

Ändern Sie Ihre Sicherheitsgruppenregeln, um den Zugriff auf bestimmte vertrauenswürdige IP-Adressen oder Bereiche einzuschränken. Denken Sie bei der Aktualisierung Ihrer Sicherheitsgruppenregeln darüber nach, die Zugriffsanforderungen für verschiedene Netzwerksegmente zu trennen, indem Sie Regeln für jeden erforderlichen Quell-IP-Bereich erstellen oder den Zugriff auf bestimmte Ports einschränken. Informationen zum Ändern von

Sicherheitsgruppenregeln finden [Sie unter Sicherheitsgruppenregeln konfigurieren](#) im EC2 Amazon-Benutzerhandbuch. Informationen zum Ändern des Standardports einer vorhandenen Amazon RDS-Datenbank-Instance finden Sie unter [Ändern des DB-Clusters mithilfe der Konsole, der CLI und der API](#) im Amazon Aurora Benutzerhandbuch.

Für die Amazon RDS-DB-Instance ist die IAM-Datenbankauthentifizierung deaktiviert

Mit der IAM-Datenbankauthentifizierung können Sie sich mit IAM-Anmeldeinformationen anstelle von Datenbankkennwörtern bei Ihrer Amazon RDS-Datenbank authentifizieren. Dies bietet mehrere Sicherheitsvorteile, wie z. B. eine zentrale Zugriffsverwaltung, temporäre Anmeldeinformationen und den Wegfall der Speicherung von Datenbankkennwörtern im Anwendungscode. Die IAM-Datenbankauthentifizierung ermöglicht die Authentifizierung von Datenbankinstanzen mit einem Authentifizierungstoken anstelle eines Kennworts. Daher wird der Netzwerkverkehr zur und von der Datenbankinstanz mit SSL verschlüsselt. Ohne IAM-Authentifizierung verlassen sich Datenbanken in der Regel auf kennwortbasierte Authentifizierung, was zur Wiederverwendung von Passwörtern und zu schwachen Passwörtern führen kann. Gemäß den bewährten Sicherheitsmethoden empfehlen wir, die IAM-Datenbankauthentifizierung zu aktivieren.

Aktivieren Sie die IAM-Datenbankauthentifizierung

Öffnen Sie in der Risikoprüfung die Ressource mit dem Hyperlink. Dadurch wird die betroffene DB-Instance geöffnet. Sie können die IAM-Datenbankauthentifizierung in den Datenbankoptionen aktivieren. Weitere Informationen finden Sie unter [Aktivieren und Deaktivieren der IAM-Datenbankauthentifizierung](#) im Amazon RDS-Benutzerhandbuch. Nachdem Sie die IAM-Authentifizierung aktiviert haben, aktualisieren Sie Ihre DB-Instances so, dass sie die IAM-Authentifizierung anstelle der kennwortbasierten Authentifizierung verwenden.

Die Amazon RDS-DB-Instance verwendet den Standard-Admin-Benutzernamen

Die Verwendung von Standardbenutzernamen (z. B. „admin“, „root“) für DB-Instances erhöht das Sicherheitsrisiko, da diese allgemein bekannt sind und häufig Ziel von Brute-Force-Angriffen sind. Standardbenutzernamen sind vorhersehbar und erleichtern es unbefugten Benutzern, sich Zugriff auf Ihre Datenbank zu verschaffen. Mit Standardbenutzernamen müssen sich Angreifer nur Passwörter beschaffen und benötigen nicht beide, um Zugriff auf Ihre Datenbank zu erhalten. Gemäß den bewährten Sicherheitsmethoden empfehlen wir, eindeutige Administrator-Benutzernamen für Ihre Datenbank-Instance zu verwenden, um die Sicherheit durch Verschleierung zu erhöhen und das Risiko unberechtigter Zugriffsversuche zu verringern.

Konfigurieren Sie einen eindeutigen Administratorbenutzernamen

Öffnen Sie in der Risikoanalyse die Ressource mit dem Hyperlink. Dadurch wird die betroffene DB-Instance geöffnet. Überlegen Sie, welche Backup-Frequenz, Aufbewahrungsdauer und Lebenszyklusregeln für Ihre Anwendungen am besten geeignet sind.

Der Amazon RDS-DB-Cluster verwendet den Standard-Admin-Benutzernamen

Die Verwendung von Standardbenutzernamen (z. B. „admin“, „root“) für DB-Instances erhöht das Sicherheitsrisiko, da diese allgemein bekannt sind und häufig Ziel von Brute-Force-Angriffen sind. Standardbenutzernamen sind vorhersehbar und erleichtern es unbefugten Benutzern, sich Zugriff auf Ihre Datenbank zu verschaffen. Mit Standardbenutzernamen müssen sich Angreifer nur Passwörter beschaffen und benötigen nicht beide, um Zugriff auf Ihre Datenbank zu erhalten. Gemäß den bewährten Sicherheitsmethoden empfehlen wir, eindeutige Administrator-Benutzernamen für Ihre Datenbank-Instance zu verwenden, um die Sicherheit durch Verschleierung zu erhöhen und das Risiko unberechtigter Zugriffsversuche zu verringern.

Konfigurieren Sie einen eindeutigen Administratorbenutzernamen

Öffnen Sie in der Risikoanalyse die Ressource mit dem Hyperlink. Dadurch wird die betroffene DB-Instance geöffnet. Sie können den Administrator-Benutzernamen einer vorhandenen Amazon RDS-DB-Instance nicht ändern. Um einen eindeutigen Administratorknamen zu erstellen, müssen Sie eine neue DB-Instance mit einem benutzerdefinierten Benutzernamen erstellen und Ihre Daten migrieren.

Für die Amazon RDS-DB-Instance sind automatische Upgrades für kleinere Versionen deaktiviert

Automatische Upgrades für Nebenversionen stellen sicher, dass Ihre Amazon RDS-Instances automatisch Upgrades für kleinere Engine-Versionen erhalten, sobald sie verfügbar sind. Diese Upgrades beinhalten häufig wichtige Sicherheitspatches und Bugfixes, die zur Aufrechterhaltung der Sicherheit und Stabilität Ihrer Datenbank beitragen. Es besteht das Risiko, dass Ihre Datenbank mit bekannten Sicherheitslücken läuft, die in neueren Nebenversionen behoben wurden. Ohne automatische Updates können sich bei Datenbankinstanzen Sicherheitslücken anhäufen, wenn neue entdeckt CVEs werden. Gemäß den bewährten Sicherheitsmethoden empfehlen wir, automatische Upgrades für kleinere Versionen für alle Amazon RDS-Instances zu aktivieren.

Aktivieren Sie automatische Upgrades für Nebenversionen

Öffnen Sie in der Risikoprüfung die Ressource mit dem Hyperlink. Dadurch wird die betroffene DB-Instance geöffnet. Sie können die Einstellungen für automatische kleinere Upgrades auf der Registerkarte Wartung und Backups einsehen. Weitere Informationen finden Sie unter [Automatische Upgrades kleinerer Versionen für Amazon RDS for MySQL](#). Sie können Ihr Wartungsfenster auch so konfigurieren, dass es in Zeiten geringer Datenbankaktivität stattfindet.

Für die Amazon RDS-DB-Instance sind automatische Backups deaktiviert

Automatisierte Backups ermöglichen die point-in-time Wiederherstellung Ihrer Amazon RDS-Instances, sodass Sie Ihre Datenbank an einem beliebigen Punkt innerhalb Ihrer Aufbewahrungsfrist wiederherstellen können. Wenn automatische Backups deaktiviert sind, riskieren Sie den Verlust von Daten im Falle eines böswilligen Löschsens, einer Datenbeschädigung oder anderer Datenverlustszenarien. Bei böswilligen Aktivitäten wie Ransomware-Angriffen, dem Löschen oder der Beschädigung von Datenbanktabellen reduziert die Möglichkeit, die Wiederherstellung zu einem Zeitpunkt vor dem Vorfall durchzuführen, die Zeit, die für die Wiederherstellung nach einem Vorfall erforderlich ist. Gemäß den bewährten Sicherheitsmethoden empfehlen wir, automatische Backups mit einer angemessenen Aufbewahrungsfrist für alle [Produktionsdatenbanken](#) zu aktivieren.

Für die Amazon RDS-DB-Instance ist der Löschschutz deaktiviert

Der Schutz vor dem Löschen von Datenbanken ist eine Funktion, die das Löschen Ihrer Datenbank-Instances verhindert. Wenn der Löschschutz deaktiviert ist, kann Ihre Datenbank von jedem Benutzer mit ausreichenden Berechtigungen gelöscht werden, was möglicherweise zu Datenverlust oder Anwendungsausfällen führen kann. Angreifer können Ihre Datenbank löschen, was zu Betriebsunterbrechungen, Datenverlust und verlängerter Wiederherstellungszeit führen kann. Gemäß den bewährten Sicherheitsmethoden empfehlen wir, den Löschschutz für Ihre RDS-DB-Instances zu aktivieren, um böswilliges Löschen zu verhindern.

Aktivieren Sie den Löschschutz für Ihren Amazon RDS-DB-Cluster

Öffnen Sie in der Risikoprüfung die Ressource mit dem Hyperlink. Dadurch wird der betroffene DB-Cluster geöffnet.

Der Löschschutz für den Amazon RDS-DB-Cluster ist deaktiviert

Der Schutz vor dem Löschen von Datenbanken ist eine Funktion, die das Löschen Ihrer Datenbank-Instances verhindert. Wenn der Löschschutz deaktiviert ist, kann Ihre Datenbank von jedem Benutzer mit ausreichenden Berechtigungen gelöscht werden, was möglicherweise zu Datenverlust oder Anwendungsausfällen führen kann. Angreifer können Ihre Datenbank löschen, was zu Betriebsunterbrechungen, Datenverlust und verlängerter Wiederherstellungszeit führen kann. Gemäß den bewährten Sicherheitsmethoden empfehlen wir, den Löschschutz für Ihre RDS-DB-Cluster zu aktivieren, um böswilliges Löschen zu verhindern.

Aktivieren Sie den Löschschutz für Ihren Amazon RDS-DB-Cluster

Öffnen Sie in der Risikoprüfung die Ressource mit dem Hyperlink. Dadurch wird der betroffene DB-Cluster geöffnet.

Die Amazon RDS-DB-Instance verwendet den Standardport für die Datenbank-Engine

Amazon RDS-Instances, die Standardports für Datenbank-Engines verwenden, können erhöhten Sicherheitsrisiken ausgesetzt sein, da diese Standardports allgemein bekannt sind und häufig von automatisierten Scan-Tools angegriffen werden. Wenn Sie Ihre DB-Instance so ändern, dass sie nicht standardmäßige Ports verwendet, wird durch Unklarheit eine zusätzliche Sicherheitsebene geschaffen, wodurch es für unbefugte Benutzer schwieriger wird, automatisierte oder gezielte Angriffe auf Ihre Datenbank durchzuführen. Standardports werden häufig von Unbefugten gesucht und können dazu führen, dass Ihre DB-Instance ins Visier genommen wird. Gemäß den bewährten Sicherheitsmethoden empfehlen wir, den Standardport durch einen benutzerdefinierten Port zu ersetzen, um das Risiko automatisierter oder gezielter Angriffe zu verringern.

Öffnen Sie in der Risikoanalyse die Ressource mit dem Hyperlink. Dadurch wird die betroffene DB-Instance geöffnet.

Aktualisieren Sie die Verbindungszeichenfolgen für die Anwendung

Nachdem Sie den Port geändert haben, aktualisieren Sie alle Anwendungen und Dienste, die eine Verbindung zu Ihrer Amazon RDS-Instance herstellen, sodass sie die neue Portnummer verwenden.

Die Amazon RDS-DB-Instance ist nicht durch einen Backup-Plan abgedeckt

AWS Backup ist ein vollständig verwalteter Backup-Service, der die Sicherung von Daten auf allen Ebenen zentralisiert und automatisiert. AWS-Services Wenn Ihre DB-Instance nicht durch einen Backup-Plan abgedeckt ist, riskieren Sie den Verlust von Daten im Falle eines böswilligen Löschens, einer Datenbeschädigung oder anderer Datenverlustszenarien. Bei böswilligen Aktivitäten wie Ransomware-Angriffen, dem Löschen oder der Beschädigung von Datenbanktabellen reduziert die Möglichkeit, die Wiederherstellung zu einem Zeitpunkt vor dem Vorfall durchzuführen, den Zeitaufwand für die Wiederherstellung nach einem Vorfall. Gemäß den bewährten Sicherheitsmethoden empfehlen wir, Ihre Amazon RDS-Instances in einen Backup-Plan aufzunehmen, um den Datenschutz zu gewährleisten.

Erstellen Sie einen Backup-Plan für Ihre DB-Instance und weisen Sie ihn zu

Öffnen Sie in der Risikoprüfung die Ressource mit dem Hyperlink. Dadurch wird die betroffene DB-Instance geöffnet. Überlegen Sie, welche Backup-Frequenz, Aufbewahrungsdauer und Lebenszyklusregeln für Ihre Anwendungen am besten geeignet sind.

Behebung von Risiken für Amazon S3 S3-Buckets

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

AWS Security Hub kann Risikopergebnisse für Amazon Simple Storage Service (S3) -Buckets generieren.

Auf der Security Hub Hub-Konsole sind der Amazon S3 S3-Bucket, der an einer Risikofeststellung beteiligt war, und seine identifizierenden Informationen im Abschnitt Ressourcen der Ergebnisdetails aufgeführt. Programmgesteuert können Sie Ressourcendetails mithilfe der [GetFindingsV2](#) Security Hub Hub-API abrufen.

Nachdem Sie die Ressource identifiziert haben, die an einer Risikofeststellung beteiligt war, können Sie die Ressource löschen, falls Sie sie nicht benötigen. Durch das Löschen einer nicht benötigten Ressource können Sie Ihr Expositionsprofil und Ihre AWS Kosten reduzieren. Wenn es sich bei der Ressource um eine wichtige Ressource handelt, befolgen Sie diese empfohlenen Abhilfemaßnahmen, um das Risiko zu minimieren. Die Themen zur Problembehebung sind nach der Art des Merkmals unterteilt.

Ein einziger Risikobefund umfasst Probleme, die in mehreren Problembehebungsthemen identifiziert wurden. Umgekehrt können Sie mit einem Problembehebungsproblem umgehen und dessen Schweregrad verringern, indem Sie sich mit nur einem Problembehebungsthema befassen. Ihr Ansatz zur Risikominderung hängt von den Anforderungen und der Arbeitsbelastung Ihres Unternehmens ab.

Note

Die in diesem Thema enthaltenen Hinweise zur Problembehebung erfordern möglicherweise zusätzliche Informationen in anderen Ressourcen. AWS

Inhalt

- [Fehlkonfigurationsmerkmale für Amazon S3 S3-Buckets](#)
 - [Für den Amazon S3 S3-Bucket ist die Versionierung deaktiviert](#)
 - [Im Amazon S3 S3-Bucket ist Object Lock deaktiviert](#)

- [Der Amazon S3 S3-Bucket ist im Ruhezustand nicht mit AWS KMS Schlüsseln verschlüsselt](#)
- [Das Löschen der Multi-Faktor-Authentifizierung \(MFA\) ist in einem versionierten Amazon S3 S3-Bucket deaktiviert](#)
- [Der Amazon S3 S3-Bucket ermöglicht es Principals anderer AWS Konten, Bucket-Berechtigungen zu ändern](#)
- [Erreichbarkeitsmerkmale für Amazon S3 S3-Buckets](#)
 - [Amazon S3 S3-Bucket hat öffentlichen Zugriff](#)
 - [Der Amazon S3 S3-Bucket hat öffentlichen Lesezugriff](#)
 - [Der Amazon S3 S3-Bucket hat Schreibzugriff](#)
 - [Für den Amazon S3 S3-Zugangspunkt sind die Einstellungen für den öffentlichen Zugriff aktiviert](#)
- [Eigenschaften sensibler Daten für Amazon S3 S3-Buckets](#)
 - [Eigenschaften sensibler Daten für Amazon S3 S3-Buckets](#)

Fehlkonfigurationsmerkmale für Amazon S3 S3-Buckets

Im Folgenden finden Sie Merkmale von Fehlkonfigurationen für Amazon S3 S3-Buckets und empfohlene Schritte zur Behebung.

Für den Amazon S3 S3-Bucket ist die Versionierung deaktiviert

Amazon S3 Versioning hilft Ihnen dabei, mehrere Varianten eines Objekts im selben Bucket zu verwalten. Wenn die Versionierung deaktiviert ist, speichert Amazon S3 nur die neueste Version jedes Objekts. Wenn Objekte versehentlich oder böswillig gelöscht oder überschrieben werden, können sie also nicht wiederhergestellt werden. Buckets mit aktivierter Versionierung bieten Schutz vor versehentlichem Löschen, Anwendungsausfällen und Sicherheitsvorfällen wie Ransomware-Angriffen, bei denen es zu unbefugten Änderungen oder Löschungen von Daten kommen kann. Gemäß den bewährten Sicherheitsmethoden empfehlen wir, die Versionierung für Buckets zu aktivieren, die wichtige Daten enthalten, deren Wiederherstellung bei Verlust schwierig oder unmöglich wäre.

1. Versionierung aktivieren — Informationen zum Aktivieren der Amazon S3 S3-Versionierung für einen Bucket finden Sie unter [Aktivieren der Versionierung für Buckets](#) im Amazon Simple Storage Service-Benutzerhandbuch. Wenn Sie die Versionierung aktivieren, sollten Sie die Implementierung von Lebenszyklusregeln zur Speicherverwaltung in Betracht ziehen, da bei der Versionierung mehrere Kopien von Objekten gespeichert werden.

Im Amazon S3 S3-Bucket ist Object Lock deaktiviert

Amazon S3 Object Lock bietet ein write-once-read-many (WORM) -Modell für Amazon S3 S3-Objekte, das verhindert, dass diese für einen bestimmten Zeitraum oder auf unbestimmte Zeit gelöscht oder überschrieben werden. Wenn Object Lock deaktiviert ist, sind Ihre Objekte möglicherweise anfällig für versehentliches oder böswilliges Löschen, Ändern oder Verschlüsseln durch Ransomware. Object Lock ist besonders wichtig für die Einhaltung gesetzlicher Anforderungen, die einen unveränderlichen Datenspeicher erfordern, und für den Schutz vor ausgeklügelten Bedrohungen wie Ransomware, die versuchen könnten, Ihre Daten zu verschlüsseln. Durch die Aktivierung von Object Lock können Sie Aufbewahrungsrichtlinien als zusätzliche Datenschutzebene durchsetzen und eine unveränderliche Backup-Strategie für Ihre kritischen Daten erstellen. Gemäß den bewährten Sicherheitsmethoden empfehlen wir Ihnen, Object Lock zu aktivieren, um böswillige Änderungen an Ihren Objekten zu verhindern.

1. Beachten Sie, dass die Objektsperre nur aktiviert werden kann, wenn Sie einen neuen Bucket erstellen. Sie müssen also einen neuen Bucket mit aktivierter Objektsperre erstellen. Erwägen Sie bei großen Migrationen die Verwendung von Batch-Operationen, um Objekte in den neuen Bucket zu kopieren. Bevor Sie Objekte sperren, müssen Sie auch Amazon S3 Versioning und Object Lock für einen Bucket aktivieren. Da Object Lock nur für neue Buckets aktiviert werden kann, müssen Sie vorhandene Daten in einen neuen Bucket migrieren, bei dem Object Lock aktiviert ist. Amazon S3 Object Lock konfigurieren — Informationen zur Konfiguration von Object Lock für einen Bucket finden Sie unter [Configuring Amazon S3 Object Lock](#) im Amazon Simple Storage Service-Benutzerhandbuch. Wählen Sie nach der Einrichtung von Object Lock einen geeigneten Aufbewahrungsmodus für Ihre Umgebung.

Der Amazon S3 S3-Bucket ist im Ruhezustand nicht mit AWS KMS Schlüsseln verschlüsselt

Amazon S3 wendet serverseitige Verschlüsselung mit verwalteten Amazon S3 S3-Schlüsseln als Standardverschlüsselungsebene für alle neuen Buckets an. Managed Keys von Amazon S3 bieten zwar einen starken Verschlüsselungsschutz, bieten jedoch nicht das gleiche Maß an Zugriffskontrolle und Auditfunktionen wie AWS Key Management Service Schlüssel. Bei Verwendung von KMS-Schlüsseln erfordert der Zugriff auf Objekte Berechtigungen sowohl für den Amazon S3 S3-Bucket als auch für den KMS-Schlüssel, mit dem das Objekt verschlüsselt wurde. Dies ist besonders wichtig für sensible Daten, bei denen Sie eine detaillierte Kontrolle darüber benötigen, wer auf die verschlüsselten Objekte zugreifen kann, und eine umfassende Auditprotokollierung der Verwendung von Verschlüsselungsschlüsseln benötigen. Gemäß den bewährten Sicherheitsmethoden empfehlen

wir die Verwendung von KMS-Schlüsseln zur Verschlüsselung von Buckets mit vertraulichen Daten oder für Umgebungen mit strengen Compliance-Anforderungen.

1. Amazon S3 S3-Bucket-Schlüssel konfigurieren

Informationen zur Konfiguration eines Buckets für die Verwendung eines Amazon S3 S3-Bucket-Schlüssels für neue Objekte finden Sie unter [Konfiguration Ihres Buckets zur Verwendung eines Amazon S3 S3-Bucket-Schlüssels mit SSE-KMS für neue Objekte](#) im Amazon Simple Storage Service-Benutzerhandbuch. Informationen zum Verschlüsseln eines vorhandenen Objekts finden Sie unter [Verschlüsseln von Objekten mit Amazon S3 Batch Operations](#) im AWS Storage-Blog.

Beachten Sie bei der Implementierung der AWS KMS Verschlüsselung Folgendes:

- **Schlüsselverwaltung** — Entscheiden Sie, ob Sie einen AWS verwalteten Schlüssel oder einen vom Kunden verwalteten Schlüssel (CMK) verwenden möchten. CMKs bieten Kunden die volle Kontrolle über den Lebenszyklus und die Verwendung ihrer Schlüssel. Weitere Informationen zum Unterschied zwischen diesen beiden Schlüsseltypen finden Sie unter [AWS KMS-Schlüssel](#) im AWS Key Management Service Entwicklerhandbuch.
- **Schlüsselrotation** — Für zusätzliche Sicherheitsmaßnahmen aktivieren Sie die automatische Schlüsselrotation für Ihre KMS-Schlüssel. Weitere Informationen finden Sie unter [Automatische Schlüsselrotation aktivieren](#) im AWS Key Management Service Entwicklerhandbuch.

Das Löschen der Multi-Faktor-Authentifizierung (MFA) ist in einem versionierten Amazon S3 S3-Bucket deaktiviert

Das Löschen mit Multi-Faktor-Authentifizierung (MFA) bietet eine zusätzliche Sicherheitsebene für Ihren Amazon S3 S3-Bucket. Für destruktive Amazon S3 S3-Operationen ist eine Multi-Faktor-Authentifizierung erforderlich. Wenn MFA Delete deaktiviert ist, können Benutzer mit entsprechenden Berechtigungen Objektversionen dauerhaft löschen oder die Versionierung in Ihrem Bucket aussetzen, ohne dass zusätzliche Authentifizierungsherausforderungen erforderlich sind. Die Aktivierung von MFA Delete schützt vor unbefugtem oder versehentlichem Löschen Ihrer Daten und bietet so einen verbesserten Schutz vor Ransomware-Angriffen, Insider-Bedrohungen und Betriebsfehlern. Die MFA-Löschung ist besonders nützlich für Buckets mit kritischen oder Compliance-sensiblen Daten, die vor unbefugtem Löschen geschützt werden müssen. Gemäß den bewährten Sicherheitsmethoden empfehlen wir, MFA für Ihre Amazon S3 S3-Buckets zu aktivieren.

1. Überprüfen Sie die MFA-Typen

AWS unterstützt die folgenden [MFA-Typen](#). Obwohl die Authentifizierung mit einem physischen Gerät in der Regel einen strengeren Sicherheitsschutz bietet, ist die Verwendung einer beliebigen Art von MFA sicherer als die Deaktivierung von MFA.

2. MFA auf der Ebene der Ressourcenrichtlinien durchsetzen

Verwenden Sie den `aws:MultiFactorAuthAge` Bedingungsschlüssel in einer Bucket-Richtlinie, um MFA für sensible Operationen vorzuschreiben. Weitere Informationen finden Sie unter [Erforderliche MFA](#) im Amazon Simple Storage Service-Benutzerhandbuch.

3. MFA aktivieren

Um MFA Delete zu aktivieren, stellen Sie zunächst sicher, dass die Versionierung in Ihrem Amazon S3 S3-Bucket aktiviert ist. Das Löschen von MFA wird nur für Buckets unterstützt, für die die Versionierung aktiviert ist. Informationen zur Aktivierung der Amazon S3 S3-Versionierung finden Sie unter [Aktivieren der Versionierung für Buckets](#) im Amazon Simple Storage Service-Benutzerhandbuch. Das Löschen von MFA kann nicht über die Amazon S3 S3-Konsole aktiviert werden. Sie müssen die Amazon S3 S3-API oder die verwenden AWS CLI. Weitere Informationen finden Sie unter [Konfiguration von MFA Delete](#) im Amazon Simple Storage Service-Benutzerhandbuch.

Der Amazon S3 S3-Bucket ermöglicht es Principals anderer AWS Konten, Bucket-Berechtigungen zu ändern

Die Amazon S3 S3-Bucket-Richtlinien steuern den Zugriff auf Buckets und Objekte. Wenn Bucket-Richtlinien es Prinzipalen anderer AWS Konten ermöglichen, Bucket-Berechtigungen zu ändern, können nicht autorisierte Benutzer Ihren Bucket neu konfigurieren. Wenn externe Hauptanmeldedaten kompromittiert werden, können unbefugte Benutzer die Kontrolle über Ihren Bucket erlangen, was zu Datenschutzverletzungen oder Serviceunterbrechungen führen kann. Gemäß den Standardsicherheitsprinzipien AWS empfiehlt es sich, die Aktionen zur Rechteverwaltung nur auf vertrauenswürdige Prinzipale zu beschränken.

1. Überprüfen und identifizieren Sie Bucket-Richtlinien

Identifizieren Sie in der Exposition den Amazon S3 S3-Bucket im ARN-Feld. Wählen Sie in der Amazon S3 S3-Konsole den Bucket aus und navigieren Sie zum Tab Permissions, um die Bucket-Richtlinie zu überprüfen. Überprüfen Sie die dem Bucket beigefügte Berechtigungsrichtlinie. Suchen Sie nach Richtlinienerklärungen, die Aktionen wie gewähren, `s3:PutBucketPolicy`,

s3:PutBucketAcl, s3:DeleteBucketPolicy, s3:* oder nach Richtlinienenerklärungen, die Prinzipalen außerhalb Ihres Kontos Zugriff gewähren, wie in der Haupteklärung angegeben.

2. Ändern Sie die Bucket-Richtlinie

Ändern Sie die Bucket-Richtlinie, um Aktionen, die anderen AWS Konten gewährt wurden, zu entfernen oder einzuschränken:

- Entfernen Sie Richtlinienenerklärungen, die externen Konten Aktionen zur Verwaltung von Berechtigungen gewähren.
- Wenn kontoübergreifender Zugriff erforderlich ist, ersetzen Sie allgemeine Berechtigungen (s3:*) durch spezifische Aktionen, die keine Verwaltung von Bucket-Berechtigungen beinhalten.

Informationen zum Ändern einer Bucket-Richtlinie finden Sie unter [Hinzufügen einer Bucket-Richtlinie mithilfe der Amazon S3 S3-Konsole](#) im Amazon S3 S3-Benutzerhandbuch.

Erreichbarkeitsmerkmale für Amazon S3 S3-Buckets

Im Folgenden finden Sie Merkmale der Erreichbarkeit für Amazon S3 S3-Buckets und empfohlene Schritte zur Problembehebung.

Amazon S3 S3-Bucket hat öffentlichen Zugriff

Standardmäßig sind Amazon S3 S3-Buckets und -Objekte privat, sie können jedoch über verschiedene Konfigurationen öffentlich gemacht werden. Wenn Sie Bucket-Richtlinien, Zugriffspunktrichtlinien oder Objektberechtigungen ändern, um öffentlichen Zugriff zu ermöglichen, riskieren Sie, sensible Daten preiszugeben.

1. Beurteilen Sie den Bereich

Beurteilen Sie anhand Ihrer Unternehmensrichtlinien, Compliance-Anforderungen oder Datenklassifizierung, ob Ihr Bucket privat gemacht werden kann. Wenn Sie nicht beabsichtigt haben, der Öffentlichkeit oder anderen Personen Zugriff auf den Bucket zu gewähren AWS-Konten, folgen Sie den übrigen Anweisungen zur Problembehebung.

2. Konfigurieren Sie den Bucket so, dass er privat ist

Wählen Sie eine der folgenden Optionen, um den privaten Zugriff für Ihren Amazon S3 S3-Bucket zu konfigurieren:

- **Kontoebene** — Informationen zum Sperren des öffentlichen Zugriffs für alle Buckets in Ihrem Konto mithilfe von Einstellungen auf Kontoebene finden Sie unter [Konfiguration der Einstellungen zum Sperren des öffentlichen Zugriffs für Ihr Konto](#) im Amazon Simple Storage Service-Benutzerhandbuch.
- **Bucket-Ebene** — Informationen zum Blockieren des öffentlichen Zugriffs für einen bestimmten Bucket finden Sie unter [Konfiguration der Einstellungen zum Blockieren des öffentlichen Zugriffs für Ihre Amazon S3-Buckets](#) im Amazon Simple Storage Service-Benutzerhandbuch.
- **Bucket-ACL oder -Richtlinien** — Informationen zum Ändern der Bucket-Zugriffskontrollliste (ACL), der Bucket-Richtlinie, der Multi-Region Access Point (MRAP) -Richtlinie oder der Zugriffspunktrichtlinie, um den öffentlichen Zugriff auf den Bucket zu entfernen, finden Sie unter [Bucket-Zugriff überprüfen und ändern](#) im Amazon Simple Storage Service-Benutzerhandbuch. Wenn Sie den öffentlichen Zugriff auf Konto- oder Bucket-Ebene blockieren, haben diese Sperren Vorrang vor einer Richtlinie, die öffentlichen Zugriff gewährt.

Der Amazon S3 S3-Bucket hat öffentlichen Lesezugriff

Amazon S3 S3-Buckets mit öffentlichem Lesezugriff ermöglichen es jedem im Internet, den Inhalt Ihres Buckets einzusehen. Dies kann zwar für öffentlich zugängliche Websites oder gemeinsam genutzte Ressourcen erforderlich sein, kann jedoch Sicherheitsrisiken mit sich bringen, wenn der Bucket sensible Daten enthält. Öffentlicher Lesezugriff kann zu unberechtigtem Ansehen und Herunterladen führen, was zu Datenschutzverletzungen führen kann, wenn sensible Daten in diesen Buckets gespeichert werden. Es wird AWS empfohlen, den Zugriff auf Amazon S3 S3-Buckets gemäß den Standardsicherheitsprinzipien auf die erforderlichen Benutzer und Systeme zu beschränken.

1. Blockieren Sie den öffentlichen Zugriff auf Bucket-Ebene

Amazon S3 bietet Einstellungen für den Block Public Access, die sowohl auf Bucket- als auch auf Kontoebene konfiguriert werden können, um öffentlichen Zugriff unabhängig von Bucket-Richtlinien oder zu verhindern ACLs. Weitere Informationen finden Sie unter [Sperren des öffentlichen Zugriffs auf Ihren Amazon S3 S3-Speicher](#) im Amazon Simple Storage Service-Benutzerhandbuch. Nachdem Sie den öffentlichen Zugriff blockiert haben, überprüfen Sie die Konfiguration Ihrer Bucket-Zugriffskontrolle, um sicherzustellen, dass sie Ihren Zugriffsanforderungen entspricht. Lesen Sie dann Ihre Amazon S3 S3-Bucket-Richtlinie, um explizit zu definieren, wer auf Ihren Bucket zugreifen kann. Beispiele für Bucket-Richtlinien finden Sie unter [Beispiele für Amazon S3 S3-Bucket-Richtlinien](#) im Amazon Simple Storage Service-Benutzerhandbuch.

2. Alternative Zugriffsmethoden

Wenn öffentlicher Lesezugriff erforderlich ist, sollten Sie diese sichereren Alternativen in Betracht ziehen:

- CloudFront— Verwendung CloudFront mit einer Origin Access Identity (OAI) oder Origin Access Control (OAC), um Lesezugriff von einem privaten Amazon S3 S3-Bucket aus zu ermöglichen. Diese Alternative schränkt den direkten Zugriff auf Ihren Amazon S3 S3-Bucket ein und ermöglicht gleichzeitig den öffentlichen Zugriff auf Inhalte über CloudFront. Weitere Informationen finden Sie unter [Beschränken des Zugriffs auf einen Amazon Amazon S3 S3-Ursprung](#) im Amazon CloudFront Developer Guide.
- Vorsigniert URLs — Verwenden Sie Presigned URLs für den temporären Zugriff auf bestimmte Objekte. Weitere Informationen finden Sie unter [Objekte mit vorsignierten Objekten teilen URLs](#) im AWSAmazon S3-Benutzerhandbuch.

Der Amazon S3 S3-Bucket hat Schreibzugriff

Amazon S3 S3-Buckets mit öffentlichem Schreibzugriff ermöglichen es jedem Benutzer im Internet, Objekte in Ihrem Bucket hochzuladen, zu ändern oder zu löschen. Dies birgt erhebliche Sicherheitsrisiken, einschließlich der Möglichkeit, dass jemand schädliche Dateien hochlädt, bestehende Dateien ändert und Daten löscht. Öffentlicher Schreibzugriff führt zu Sicherheitslücken, die von Angreifern ausgenutzt werden können. Gemäß den Standardsicherheitsprinzipien wird AWS empfohlen, den Schreibzugriff auf Ihre Amazon S3 S3-Buckets auf die erforderlichen Benutzer und Systeme zu beschränken.

1. Blockieren Sie den öffentlichen Zugriff auf Konto- und Bucket-Ebene

Amazon S3 bietet Einstellungen zum Blockieren des öffentlichen Zugriffs, die sowohl auf Bucket- als auch auf Kontoebene konfiguriert werden können, um öffentlichen Zugriff unabhängig von Bucket-Richtlinien oder zu verhindern ACLs. Weitere Informationen finden Sie unter [Sperren des öffentlichen Zugriffs auf Ihren Amazon S3 S3-Speicher](#) im Amazon Simple Storage Service-Benutzerhandbuch.

2. Bucket-Richtlinien ändern

Einen detaillierteren Ansatz zum Entfernen des öffentlichen Schreibzugriffs finden Sie in der Bucket-Richtlinie. Sie können nach `s3:PutObjects3:DeleteObject`, oder `s3:*` suchen. Weitere Informationen zur Verwaltung von Bucket-Richtlinien finden Sie unter [Bucket-Richtlinien für Amazon S3](#) im Amazon Simple Storage Service-Benutzerhandbuch.

3. Alternative Zugriffsmethoden Wenn öffentlicher Lesezugriff erforderlich ist, sollten Sie diese sichereren Alternativen in Betracht ziehen:

- CloudFront— Verwendung CloudFront mit einer Origin Access Identity (OAI) oder Origin Access Control (OAC), um Lesezugriff von einem privaten Amazon S3 S3-Bucket aus zu ermöglichen. Diese Alternative schränkt den direkten Zugriff auf Ihren Amazon S3 S3-Bucket ein und ermöglicht gleichzeitig den öffentlichen Zugriff auf Inhalte über CloudFront. Weitere Informationen finden Sie unter [Beschränken des Zugriffs auf einen Amazon S3 S3-Ursprung](#) im Amazon CloudFront Developer Guide.
- Vorsigniert URLs — Verwenden Sie Presigned URLs für den temporären Zugriff auf bestimmte Objekte. Weitere Informationen finden Sie unter [Freigeben von Objekten mit URLs Vorsignierung](#) im Amazon Simple Storage Service-Benutzerhandbuch.

Für den Amazon S3 S3-Zugangspunkt sind die Einstellungen für den öffentlichen Zugriff aktiviert

Amazon S3 S3-Zugriffspunkte bieten maßgeschneiderten Zugriff auf gemeinsam genutzte Datensätze in Amazon S3 S3-Buckets. Wenn Sie den öffentlichen Zugriff für einen Access Point aktivieren, kann jeder im Internet auf Ihre Daten zugreifen. Es wird AWS empfohlen, den öffentlichen Zugriff auf Amazon S3 S3-Zugriffspunkte gemäß den Standardsicherheitsprinzipien einzuschränken.

1. Erstellen Sie einen neuen Access Point mit aktivierter Option „Öffentlichen Zugriff blockieren“

Amazon S3 unterstützt nicht, die Einstellungen für den öffentlichen Zugriff eines Access Points zu ändern, nachdem ein Access Point erstellt wurde. Informationen zum Erstellen eines Access Points finden Sie unter [Verwaltung des öffentlichen Zugriffs auf Access Points für allgemeine Zwecke](#) im Amazon S3 S3-Benutzerhandbuch. Weitere Informationen zur Verwaltung des öffentlichen Zugriffs auf Access Points finden Sie unter [Creating Access Points for General Purpose Buckets](#) im Amazon S3 S3-Benutzerhandbuch.

Eigenschaften sensibler Daten für Amazon S3 S3-Buckets

Im Folgenden finden Sie die Merkmale sensibler Daten für Amazon S3 S3-Buckets und empfohlene Schritte zur Problembehebung.

Eigenschaften sensibler Daten für Amazon S3 S3-Buckets

Wenn Macie sensible Daten in Ihren Amazon S3 S3-Buckets identifiziert, deutet dies auf potenzielle Sicherheits- und Compliance-Risiken hin, die sofortige Aufmerksamkeit erfordern.

Zu den sensiblen Daten können gehören:

- Anmeldeinformationen
- Persönlich identifizierbare Informationen
- Finanzinformationen
- Vertraulicher Inhalt, der geschützt werden muss

Wenn sensible Daten durch Fehlkonfigurationen oder unbefugten Zugriff offengelegt werden, kann dies zu Compliance-Verstößen, Datenschutzverletzungen, Identitätsdiebstahl oder finanziellen Verlusten führen. Befolgt bewährte Sicherheitsmethoden und AWS empfiehlt die korrekte Klassifizierung von Daten und die kontinuierliche Überwachung sensibler Daten in Ihren Amazon S3 S3-Buckets.

Implementieren Sie Kontrollen für sensible Daten

Wählen Sie in der Expositionsanalyse die Option Ressource öffnen aus. Überprüfen Sie den Typ der erkannten sensiblen Daten und deren Position im Bucket. Hilfe bei der Interpretation von Macie-Ergebnissen finden Sie unter [Typen von Macie-Ergebnissen](#) im Amazon Macie Macie-Benutzerhandbuch.

Implementieren Sie je nach Art der entdeckten sensiblen Daten die entsprechenden Sicherheitskontrollen:

- Beschränken Sie den Zugriff auf den Bucket — Überprüfen Sie die Bucket-Berechtigungen, um sicherzustellen, dass sie dem Prinzip der geringsten Rechte entsprechen. Verwenden Sie IAM-Richtlinien, Bucket-Richtlinien und ACLs um den Zugriff einzuschränken. Weitere Informationen finden Sie unter [Identity and Access Management für Amazon S3](#) im Amazon Simple Storage Service-Benutzerhandbuch.
- Serverseitige Verschlüsselung aktivieren — Aktivieren Sie serverseitige Verschlüsselung mit KMS-Schlüsseln für zusätzlichen Schutz. Weitere Informationen finden Sie unter [Verwenden der serverseitigen Verschlüsselung mit AWS KMS-Schlüsseln \(SSE-KMS\)](#) im Amazon Simple Storage Service-Benutzerhandbuch.
- Verwendung AWS Glue DataBrew — Wird Glue DataBrew zur Datenvorbereitung und -bereinigung verwendet. Weitere Informationen finden Sie unter [Was ist AWS Glue DataBrew](#) im AWS Glue DataBrew Entwicklerhandbuch enthalten.

Ergebnisse der Angriffssequenz im Security Hub

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

Eine [Angriffssequenz](#) ist eine Art von Sicherheitsbedrohung. GuardDuty generiert Ergebnisse für Angriffssequenzen, wenn Ereignisse mit einem Muster verdächtiger Aktivitäten übereinstimmen. Wenn Sie diese [Option aktivieren GuardDuty](#), können Sie in der Security Hub Hub-Konsole auf diese Art von Suche zugreifen. Auf diese Weise können Sie alle Ihre Sicherheitsbedrohungen untersuchen und beheben, ohne die Konsole wechseln zu müssen. Sie können Ihre Ergebnisse zur Angriffssequenz auf dem Bildschirm Bedrohungen der Security Hub Hub-Konsole überprüfen.

Überprüfung der Ergebnisse zur Angriffssequenz

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

Sie können Ihre Ergebnisse zur Angriffssequenz auf dem Bildschirm Bedrohungen der Security Hub Hub-Konsole überprüfen. Im folgenden Thema wird beschrieben, wie Sie die Details einer gefundenen Angriffssequenz überprüfen.

Überprüfung der Einzelheiten zu den Ergebnissen der Angriffssequenz

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

In diesem Thema wird beschrieben, wie Sie Details zu den Ergebnissen der Angriffssequenz in der Security Hub Hub-Konsole und mit der API überprüfen können.

Details zu Angriffssequenzen in der Security Hub Hub-Konsole überprüfen

Im Folgenden wird beschrieben, wie Sie Details zu Angriffssequenzen in der Security Hub Hub-Konsole überprüfen können:

Um die Ergebnisse der Angriffssequenz in der Konsole zu überprüfen

1. Melden Sie sich mit Ihren Anmeldeinformationen an und öffnen Sie die Security Hub Hub-Konsole unter <https://console.aws.amazon.com/securityhub/v2/home? region=us-ost-1>.
2. Wählen Sie im Navigationsbereich die Option Bedrohungen aus.
3. Wählen Sie aus der Liste der Ergebnisse der Angriffssequenz das Ergebnis der Angriffssequenz aus, für das Sie Details anzeigen möchten.

Überprüfen Sie die Details zu den Ergebnissen der Angriffssequenz mit der API

Sie können die Ergebnisse der Angriffssequenz mit der [GetFindingsV2API](#) oder der überprüfen AWS CLI. Sie können Ergebnisse mit dem [FindingProviderFields](#)Parameter filtern und den Filterwert angeben, TTPs/AttackSequence wenn Sie nur Ergebnisse der Angriffssequenz zurückgeben möchten. Sie können nach anderen Feldern filtern, um die Ergebnisse einzugrenzen.

-Beispielbefehl

Im Folgenden finden Sie ein AWS CLI Beispiel, das die 10 zuletzt generierten Ergebnisse der Angriffssequenz in Ihrem Konto abrufen. Das Beispiel ist für Linux, macOS und Unix formatiert, und der umgekehrte Schrägstrich (\) wird verwendet, um die Lesbarkeit zu verbessern.

```
$ aws securityhub get-findings-v2 \
--filters '{"FindingProviderFieldsTypes":[{"Value": "TTPs/AttackSequence", "Comparison": "PREFIX"}]}' \
--sort-criteria '{ "Field": "LastObservedAt", "SortOrder": "desc" }' \
--max-items 10
```

Behebung von Ergebnissen der Angriffssequenz

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

Informationen zur Behebung von Ergebnissen der Angriffssequenz finden Sie unter [Behebung erkannter GuardDuty Sicherheitslücken](#) im GuardDuty Amazon-Benutzerhandbuch.

Automatisierungsregeln in Security Hub

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

Security Hub-Automatisierungsregeln sind eine erweiterbarere und konfigurierbarere Version der [Security Hub CSPM-Automatisierungsregeln](#). Security Hub entwickelte sich von einem erkenntungsspezifischen Automatisierungssystem zu einer breiteren Konfigurationsplattform. Während Security Hub CSPM ASFF unterstützt, bietet Security Hub Unterstützung für OCSF und schafft eine Grundlage für mehr Konfigurationen. Eines der Hauptmerkmale der Automatisierungsregeln für Security Hub ist die Integration in die Aggregatorkonfiguration. Dies bietet die Möglichkeit, Konfigurationen fein abzustimmen und granular für eine Reihe von verknüpften Konfigurationen bereitzustellen, wobei AWS-Regionen gleichzeitig die Flexibilität erhalten bleibt, regionale Erfahrungen einzurichten, indem einzelne Konfigurationen getrennt AWS-Regionen werden.

Security Hub Hub-Ressourcen in Ihrer AWS-Konto AWS-Region Hand, einschließlich Automatisierungsregeln, Konnektoren und Aggregatoren, funktionieren in den folgenden Szenarien nicht mehr.

- Der Standalone-Computer AWS-Konto wird Mitglied einer AWS Organisation mit einem delegierten Administrator
- Das AWS Organisationsverwaltungskonto entfernt den delegierten Administrator für die Organisation und richtet einen neuen delegierten Administrator ein
- Die Aggregatorkonfiguration des delegierten Administrators oder des eigenständigen Administrators AWS-Konto wird geändert, sodass aus einer Region ohne Verknüpfung eine verknüpfte Region wird

In diesen Szenarien kann das Mitgliedskonto diese Ressourcen weiterhin über die Vorgänge Auflisten, Abrufen und Löschen verwalten. AWS CLI Wenn eine nicht verknüpfte Region zu einer verknüpften Region gemacht wird, kann der delegierte Administrator oder das eigenständige AWS Konto die alten Ressourcen in einer verknüpften Region weiterhin über die Operationen Auflisten, Abrufen und Löschen verwalten.

Wichtigste Verbesserungen

Die Automatisierungsregeln in Security Hub CSPM sind regional und gelten nur für Ergebnisse dort, AWS-Regionen wo sie erstellt wurden. Automatisierungsregeln in Security Hub können einmal in einer AWS-Region (Aggregationsregion) konfiguriert und dann über die Aggregator V2-Einstellung auf alle konfigurierten AWS-Regionen (verknüpften Regionen) angewendet werden. Ein Vorteil dieser Funktion ist die Möglichkeit, mehrere Sicherheitslücken zu automatisieren und zu korrigieren, indem AWS-Regionen nur eine eingerichtet wird. AWS-Region Das heißt, wenn ein Ergebnis in einer verknüpften Region generiert wird, kann es auf der Grundlage der Konfiguration der Aggregationsregion automatisch behoben werden.

Externe Integration

Automatisierungsregeln in Security Hub unterstützen einen Aktionstyp für die Erstellung von ITSM-Tickets. Auf diese Weise können Kunden ausgewählte OCSF-Ergebnisse direkt an eine oder mehrere konfigurierte ITSM-Integrationen weiterleiten. Wenn ein OCSF-Ergebnis den Kriterien entspricht, können Sie ein Ticket in oder erstellen. Jira Cloud ServiceNow ITSM Weitere Informationen finden Sie unter [Integrationen von Drittanbietern für Security Hub](#).

Von OCSF unterstützte Kriterien

Security Hub CSPM unterstützt die Bewertung von ASFF-Feldern anhand von Ergebnissen, während Security Hub OCSF-Felder abgleicht. Beispielsweise entspricht der Satz unterstützter Filter für den in V2-Automatisierungsregeln verwendeten `Criteria` Parameter dem Satz unterstützter Filter für den `Criteria` in verwendeten Parameter. [GetFindingsV2](#) Das bedeutet, dass Filter, die zum Abrufen von V2-Ergebnissen verwendet werden, in einer V2-Automatisierungsregel verwendet werden können, die den Ergebnissen entspricht.

OCSF-Felder für die **AutomationRulesFindingFieldsUpdate**

Die Liste der Felder, für die [AutomationRulesFindingFieldsUpdate](#) in Security Hub CSPM aktualisiert werden können, wurde in Security Hub geändert.

[AutomationRulesFindingFieldsUpdateV2](#) Die Liste der Felder, die aktualisiert werden können, umfasst Folgendes:

- `Comment`
- `SeverityId`

- StatusId

Integrationen von Drittanbietern für Security Hub

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

Sie können Ihre Sicherheitslage mit Integrationen von Drittanbietern für AWS Security Hub verbessern. Mit dieser Funktion können Sie Integrationen aktivieren, die Erkenntnisse aus Security Hub nutzen, sodass Sie Ihre Betriebs-, Untersuchungs- und Reaktionstools in Security Hub integrieren können. Derzeit unterstützt Security Hub die Integration mit Jira Cloud und ServiceNow.

Erstellen Sie einen KMS-Schlüssel, um Anmeldeinformationen zu verschlüsseln

Die Integrationsverfahren in diesem Abschnitt bieten Ihnen die Möglichkeit, Ihre Anmeldeinformationen mit einem AWS eigenen Schlüssel oder einem vom Kunden verwalteten Schlüssel zu verschlüsseln. Ein AWS eigener Schlüssel ist ein KMS-Schlüssel, der sich nicht in Ihrem befindet, AWS-Konto da der AWS Dienst, der Ihre Anmeldeinformationen verschlüsselt, den KMS-Schlüssel besitzt und verwaltet. Wenn Sie die vollständige Kontrolle über den KMS-Schlüssel haben möchten, der zur Verschlüsselung Ihrer Anmeldeinformationen verwendet wird, [erstellen Sie einen vom Kunden verwalteten](#) Schlüssel. Ein vom Kunden verwalteter Schlüssel ist ein KMS-Schlüssel, den Sie besitzen und verwalten.

Zugriff auf Security Hub Hub-Verschlüsselungsvorgänge

Diese Richtlinienerklärung ermöglicht es Security Hub, den AWS KMS Schlüssel für Verschlüsselungsvorgänge zu verwenden. Es ermöglicht Security Hub, Ihre Kundengeheimnisse mit diesem Schlüssel zu schützen. Die Berechtigungen sind über den Bedingungsblock, der den Quell-ARN und den Verschlüsselungskontext überprüft, auf Vorgänge im Zusammenhang mit bestimmten Security Hub Hub-Connectoren beschränkt.

```
{
  "Sid": "Allow Security Hub access to the customer managed key",
  "Effect": "Allow",
  "Principal": {
```

```

    "Service": "connector.securityhub.amazonaws.com"
  },
  "Action": [
    "kms:GenerateDataKey",
    "kms:Decrypt",
    "kms:ReEncrypt*"
  ],
  "Resource": "*",
  "Condition": {
    "ArnLike": {
      "aws:SourceArn": "arn:aws:securityhub:${Region}:${AccountId}:connectorv2/*"
    },
    "StringLike": {
      "kms:EncryptionContext:aws:securityhub:connectorV2Arn":
"arn:aws:securityhub:${Region}:${AccountId}:connectorv2/*",
      "kms:EncryptionContext:aws:securityhub:providerName":
"${CloudProviderName}"
    }
  }
}

```

Note

Geben Sie für *CloudProviderName* JIRA_CLOUD oder einSERVICENOW. Geben Sie für *Region* AWS-Region und *AccountId* Ihre AWS-Konto ID ein.

Security Hub Hub-Schlüssellesezugriff

Diese Richtlinienerklärung ermöglicht es Security Hub, Metadaten über den KMS-Schlüssel zu lesen, indem der DescribeKey Vorgang zugelassen wird. Diese Berechtigung ist erforderlich, damit Security Hub den Status und die Konfiguration des Schlüssels überprüfen kann. Der Zugriff ist über die ARN-Quellbedingung auf bestimmte Security Hub Hub-Konnektoren beschränkt.

```

{
  "Sid": "Allow Security Hub read access to the customer managed key",
  "Effect": "Allow",
  "Principal": {
    "Service": "connector.securityhub.amazonaws.com"
  },
  "Action": [
    "kms:DescribeKey"
  ]
}

```

```

    ],
    "Resource": "*",
    "Condition": {
        "ArnLike": {
            "aws:SourceArn": "arn:aws:securityhub:${Region}:${AccountId}:connectorv2/*"
        }
    }
}

```

Note

Geben Sie für *Region* *AccountId* AWS-Region und Ihre AWS-Konto UND-ID ein.

IAM-Prinzipalzugriff für Security Hub Hub-Operationen

Diese Richtlinienerklärung gewährt der angegebenen IAM-Rolle Berechtigungen zur Ausführung wichtiger Operationen (Beschreiben, Generieren, Entschlüsseln, erneuten Verschlüsseln und Auflisten von Aliasen), wenn sie mit Security Hub über V2 und V2 interagieren. [CreateConnector](#) [CreateTicket](#) APIs Die Bedingung stellt sicher, dass diese Operationen nur über den Security Hub Hub-Dienst in der angegebenen Region ausgeführt werden können.

```

{
    "Sid": "Allow permissions to access key through Security Hub",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::${AccountId}:role/${RoleName}"
    },
    "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt",
        "kms:ReEncrypt*"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:ViaService": [
                "securityhub.${Region}.amazonaws.com"
            ]
        },
        "StringLike": {
            "kms:EncryptionContext:aws:securityhub:providerName": "SERVICENOW"
        }
    }
}

```

```
    }
  }
}

{
  "Sid": "Allow read permissions to access key through Security Hub",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::${AccountId}:role/${RoleName}"
  },
  "Action": [
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": [
        "securityhub.${Region}.amazonaws.com"
      ]
    }
  }
}
```

Note

Geben Sie für *RoleName* den Namen der IAM-Rolle ein, die Security Hub aufruft. Geben Sie für *Region* AWS-Region und *AccountId* Ihre AWS-Konto ID ein.

Integrationen für AWS Security Hub Jira Cloud

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

In diesem Thema wird beschrieben, wie Sie auf die Security Hub Hub-Konsole zugreifen, um eine Integration für zu konfigurieren Jira Cloud. Bevor Sie eines der Verfahren in diesem Thema abschließen können, müssen Sie ein Jira Cloud Abonnement erwerben. Informationen zu Abonnementplänen finden Sie auf der Atlassian Website unter [Preise](#).

Für Konten in einer Organisation kann nur der delegierte Administrator eine Integration konfigurieren. Der delegierte Administrator kann die Funktion „Ticket erstellen“ manuell für alle Ergebnisse zu Mitgliedskonten verwenden. Darüber hinaus kann der delegierte Administrator mithilfe von [Automatisierungsregeln](#) automatisch Tickets für alle Ergebnisse im Zusammenhang mit Mitgliedskonten erstellen. Bei der Definition einer Automatisierungsregel kann der delegierte Administrator Kriterien festlegen, die alle Mitgliedskonten oder bestimmte Mitgliedskonten umfassen können. Informationen zum Einrichten eines delegierten Administrators finden Sie unter [Ein delegiertes Administratorkonto in Security Hub](#) einrichten.

Für Konten, die nicht zu einer Organisation gehören, sind alle Aspekte dieser Funktion verfügbar.

Voraussetzungen

Sie müssen die folgenden Voraussetzungen erfüllen, bevor Sie eine Integration für konfigurieren können Jira Cloud. Andernfalls funktioniert Ihre Integration zwischen Jira Cloud und Security Hub nicht.

1. Installieren Sie den AWS Security Hub für die Jira Cloud App

Das folgende Verfahren beschreibt, wie Sie die App installieren.

1. Melden Sie sich als Administrator Atlassian auf Ihrer Site an.
2. Wählen Sie Einstellungen und dann Apps.
3. Wenn Sie zur Marketplace-Seite weitergeleitet werden, wählen Sie Neue Apps suchen aus. Wenn Sie zur Apps-Seite weitergeleitet werden, wählen Sie Apps entdecken und suchen Sie dann nach AWS Security Hub für Jira Cloud. Wählen Sie dann Jetzt herunterladen.

2. Erstellen eines Projekts

Dieser Schritt ist erforderlich, wenn Sie kein Projekt erstellt haben. Informationen zum Erstellen eines Projekts finden Sie in der Jira Cloud Support Dokumentation unter [Neues Projekt erstellen](#).

Voraussetzungen für die Erstellung eines Projekts

Stellen Sie sicher, dass Sie beim Erstellen eines neuen Projekts Folgendes beachten.

- Wählen Sie Softwareentwicklung für die Projektvorlage aus.
- Wählen Sie für den Projekttyp „Vom Unternehmen verwaltet“ aus.

- Notieren Sie sich den Projektschlüssel.

3. Fügen Sie Ihre Softwareentwicklungsprojekte zum AWS Security Hub for Jira Cloud App hinzu

Das folgende Verfahren beschreibt, wie Sie Ihre Softwareentwicklungsprojekte zum Security Hub for Jira Cloud App hinzufügen.

1. Melden Sie sich als Administrator Atlassian auf Ihrer Site an.
2. Wählen Sie Einstellungen und dann Apps.
3. Wählen Sie in der Liste der Apps AWS Security Hub for Jira Cloud aus.
4. Wählen Sie den Tab Connector-Einstellungen.
5. Wählen Sie unter Aktivierte Projekte die Option Jira-Projekt hinzufügen aus.
 - a. Wählen Sie in der Dropdownliste die Option Alle hinzufügen oder wählen Sie ein Projekt aus. Wiederholen Sie diesen Teil des Schritts, wenn Sie mehr als ein Projekt hinzufügen möchten, aber nicht alle Projekte.
 - b. Wählen Sie Speichern.

Auf der Registerkarte Installation Manager können Sie überprüfen, welche Projekte erfolgreich installiert wurden. Auf der Registerkarte Installation Manager können Sie auch Konfigurationen für Felder, Bildschirme, Status und Workflows überprüfen.

Note

Sie können die Registerkarte Installation Manager wählen, um zu überprüfen, ob alle ausgewählten Projekte erfolgreich installiert wurden.

Weitere Informationen Jira Cloud dazu finden Sie in den [Jira Cloud Ressourcen](#) auf der Atlassian Website.

Empfehlungen

Im Folgenden finden Sie Empfehlungen, die Sie berücksichtigen sollten, bevor Sie eine Integration für konfigurieren Jira Cloud.

- Erstellen Sie ein spezielles Systemkonto in Jira Cloud.

- Verwenden Sie ein Systemkonto pro Jira Cloud Instanz.

Konfigurieren Sie eine Integration für Jira Cloud

Security Hub erstellt automatisch Probleme in Jira Cloud. Diese Integration ermöglicht es Ihnen, Security Hub Hub-Ergebnisse an zu senden Jira Cloud, sodass Sie sie als Teil Ihrer betrieblichen Workflows verwalten können. Sie können beispielsweise Problemen, die untersucht und behoben werden müssen, die Verantwortung zuweisen. Sie müssen das folgende Verfahren für jedes Ihrer Jira Cloud Projekte ausführen, an das Sie Security Hub Hub-Ergebnisse senden möchten.

Note

Wenn Sie einen Jira Cloud Connector erstellen, werden Sie vom aktuellen AWS-Region zu weitergeleitet "<https://3rdp.oauth.console.aws>", sodass Sie die Connector-Registrierung abschließen können. Danach kehren Sie zu dem Ort zurück, AWS-Region an dem der Konnektor erstellt wird.

Um eine Integration zu konfigurieren für Jira Cloud

1. Melden Sie sich mit Ihren Zugangsdaten bei Ihrem AWS Konto an und öffnen Sie die Security Hub Hub-Konsole unter <https://console.aws.amazon.com/securityhub/v2/home?region=us-ost-1>.
2. Wählen Sie im Navigationsbereich Management und dann Integrationen aus.
3. Wählen Sie Hinzufügen Jira Cloud aus.
4. Geben Sie unter Details einen eindeutigen und aussagekräftigen Namen für Ihre Integration ein und legen Sie fest, ob Sie eine optionale Beschreibung für Ihre Integration eingeben möchten.
5. Entscheiden Sie unter Sicherheitseinstellungen, wie Sie Ihre Jira Cloud Anmeldeinformationen in Security Hub verschlüsseln möchten. Wenn Sie sich für den Service Owned Key entscheiden, wird ein AWS eigener Schlüssel zur Verschlüsselung Ihrer Daten verwendet. Wenn Sie Benutzerdefinierter Schlüssel wählen, müssen Sie den ARN für einen vorhandenen benutzerdefinierten Schlüssel eingeben oder einen neuen Schlüssel erstellen, indem Sie AWS KMS Schlüssel erstellen wählen. Informationen zum Erstellen eines KMS-Schlüssels finden Sie unter [Erstellen eines KMS-Schlüssels mit symmetrischer Verschlüsselung](#).

 Note

Sie können diese Einstellungen nicht mehr ändern, nachdem Sie diese Konfiguration abgeschlossen haben. Wenn Sie jedoch Benutzerdefinierter Schlüssel wählen, können Sie Ihre benutzerdefinierte Schlüsselrichtlinie jederzeit bearbeiten.

6. (Optional) Erstellen Sie für Tags ein Tag und fügen Sie es Ihrer Integration hinzu. Sie können bis zu 50 Tags hinzufügen.
7. Wählen Sie für Autorisierungen die Option Connector erstellen und autorisieren aus. Es erscheint ein Pop-up, in dem Sie Zulassen wählen, um die Autorisierung abzuschließen. Nachdem Sie die Autorisierung abgeschlossen haben, wird ein Kontrollkästchen angezeigt, das Sie darüber informiert, dass die Autorisierung erfolgreich war.
8. Geben Sie für Konfigurationen die Jira Cloud Projekt-ID ein.
9. Wählen Sie Vollständige Konfiguration aus. Nachdem Sie die Konfiguration abgeschlossen haben, können Sie Ihre konfigurierten Integrationen auf der Registerkarte Konfigurierte Integrationen einsehen.

Ein Ticket für eine Integration erstellen Jira Cloud

 Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

Nachdem Sie eine Integration mit erstellt haben Jira Cloud, können Sie ein Ticket für einen Befund erstellen.

 Note

Ein Ergebnis wird während seines gesamten Lebenszyklus immer einem einzelnen Ticket zugeordnet. Alle nachfolgenden Aktualisierungen eines Ergebnisses nach der ersten Erstellung werden an dasselbe Ticket gesendet. Wenn ein mit einer Automatisierungsregel verknüpfter Connector geändert wird, wird der aktualisierte Connector nur für neue und eingehende Ergebnisse verwendet, die den Regelkriterien entsprechen.

Um ein Ticket für einen Befund zu erstellen

1. Melden Sie sich mit Ihren Zugangsdaten bei Ihrem AWS Konto an und öffnen Sie die Security Hub Hub-Konsole unter <https://console.aws.amazon.com/securityhub/v2/home? region=us-ost-1>.
2. Wählen Sie im Navigationsbereich unter Inventar die Option Findings aus.
3. Wählen Sie einen Befund aus. Wählen Sie im Ergebnis die Option Ticket erstellen aus.
4. Öffnen Sie für Integration das Drop-down-Menü und wählen Sie eine Integration aus. Diese Integration ist die Integration, die Sie zuvor bei der Konfiguration des Jira Cloud Projekts erstellt haben. Wählen Sie die Integration aus, an die die Ergebnisse gesendet werden sollen.
5. Wählen Sie Erstellen aus.

Ein Ticket für eine Jira Cloud Integration anzeigen

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

Nachdem Sie ein Ticket für einen Befund erstellt haben, können Sie das Ticket auf Ihrer Jira Cloud Instanz öffnen.

Um einen Befund auf deiner Jira Cloud Instanz zu sehen

1. Melden Sie sich mit Ihren Zugangsdaten bei Ihrem AWS Konto an und öffnen Sie die Security Hub Hub-Konsole unter <https://console.aws.amazon.com/securityhub/v2/home? region=us-ost-1>.
2. Wählen Sie im Navigationsbereich unter Inventar die Option Findings aus.
3. Wählen Sie die Suche aus, in der Sie das Ticket erstellt haben.
4. Wählen Sie in der Suche die Ticket-ID aus, um das Ticket auf Ihrer Jira Cloud Instanz anzuzeigen, oder wählen Sie „JSON anzeigen“ aus.

Integrationen für ServiceNow

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

In diesem Thema wird beschrieben, wie Sie auf die Security Hub Hub-Konsole zugreifen, um eine Integration für zu konfigurierenServiceNow ITSM. Bevor Sie eines der Verfahren in diesem Thema abschließen können, müssen Sie über ein Abonnement verfügen, ServiceNow ITSM bevor Sie diese Integration hinzufügen können. Weitere Informationen finden Sie auf [der Seite mit den Preisen](#) auf der ServiceNow Website.

Für Konten in einer Organisation kann nur der delegierte Administrator eine Integration konfigurieren. Der delegierte Administrator kann die Funktion „Ticket erstellen“ manuell für alle Ergebnisse zu Mitgliedskonten verwenden. Darüber hinaus kann der delegierte Administrator mithilfe von [Automatisierungsregeln](#) automatisch Tickets für alle Ergebnisse im Zusammenhang mit Mitgliedskonten erstellen. Bei der Definition einer Automatisierungsregel kann der delegierte Administrator Kriterien festlegen, die alle Mitgliedskonten oder bestimmte Mitgliedskonten umfassen können. Informationen zum Einrichten eines delegierten Administrators finden Sie unter [Ein delegiertes Administratorkonto in Security Hub](#) einrichten.

Für Konten, die nicht zu einer Organisation gehören, sind alle Aspekte dieser Funktion verfügbar.

Voraussetzungen

Sie müssen die folgenden Voraussetzungen erfüllen, bevor Sie eine Integration für konfigurieren könnenServiceNow ITSM. Andernfalls funktioniert Ihre Integration zwischen ServiceNow ITSM und Security Hub nicht.

1. Installieren Sie die Security Hubfinds-Integration für IT Service Management (ITSM)

Das folgende Verfahren beschreibt, wie das Security Hub-Plugin installiert wird.

1. Melden Sie sich bei Ihrer ServiceNow ITSM Instance an und öffnen Sie dann den Anwendungsnavigator.
2. Navigieren Sie zum [ServiceNow Store](#).
3. Suchen Sie nach Security Hub Findings Integration for IT Service Management (ITSM) und wählen Sie dann Get, um die Anwendung zu installieren.

Note

Wählen Sie in den Einstellungen für die Security Hub Hub-Anwendung aus, welche Aktion ausgeführt werden soll, wenn neue Security Hub Hub-Ergebnisse an Ihre ServiceNow ITSM

Umgebung gesendet werden. Sie können „Nichts tun“, „Vorfall erstellen“, „Problem erstellen“ oder „Beides erstellen“ wählen (Vorfall/Problem)

2. Konfigurieren Sie den Gewährungstyp „Client-Anmeldeinformationen“ für eingehende Anfragen OAuth

Sie müssen diesen Gewährungstyp für eingehende OAuth Anfragen konfigurieren. Weitere Informationen finden Sie auf der ServiceNow Support-Webseite unter Die [Art der Gewährung von Kundenanmeldeinformationen für eingehende Anrufe OAuth wird unterstützt](#).

3. Erstellen Sie eine Anwendung OAuth

Wenn Sie bereits eine OAuth Anwendung erstellt haben, können Sie diese Voraussetzung überspringen. Informationen zum Erstellen einer OAuth Anwendung finden Sie unter [Einrichtung OAuth](#).

Konfigurieren Sie eine Integration für ServiceNow ITSM

Security Hub kann Vorfälle oder Probleme automatisch in erstellenServiceNow ITSM.

Um eine Integration zu konfigurieren für ServiceNow ITSM

1. Melden Sie sich mit Ihren Zugangsdaten bei Ihrem AWS Konto an und öffnen Sie die Security Hub Hub-Konsole unter <https://console.aws.amazon.com/securityhub/v2/home? region=us-ost-1>.
2. Wählen Sie im Navigationsbereich Management und dann Integrationen aus.
3. Wählen Sie ServiceNow ITSMunter Integration hinzufügen aus.
4. Geben Sie unter Details einen Namen für Ihre Integration ein und legen Sie fest, ob Sie eine optionale Beschreibung für Ihre Integration eingeben möchten.
5. Entscheiden Sie unter Sicherheitseinstellungen, wie Sie Ihre Jira Cloud Anmeldeinformationen in Security Hub verschlüsseln möchten. Wenn Sie sich für den Service Owned Key entscheiden, wird ein AWS eigener Schlüssel zur Verschlüsselung Ihrer Daten verwendet. Wenn Sie Benutzerdefinierter Schlüssel wählen, müssen Sie den ARN für einen vorhandenen benutzerdefinierten Schlüssel eingeben oder einen neuen Schlüssel erstellen, indem Sie AWS KMS Schlüssel erstellen wählen. Informationen zum Erstellen eines KMS-Schlüssels finden Sie unter [Erstellen eines KMS-Schlüssels mit symmetrischer Verschlüsselung](#).

 Note

Sie können diese Einstellungen nicht mehr ändern, nachdem Sie diese Konfiguration abgeschlossen haben. Wenn Sie jedoch Benutzerdefinierter Schlüssel wählen, können Sie Ihre benutzerdefinierte Schlüsselrichtlinie jederzeit bearbeiten.

6. Geben Sie für Autorisierungen ServiceNow ITSM URL, Client-ID und Client Secret ein.
7. Legen Sie für Tags fest, ob Sie ein optionales Tag erstellen und zu Ihrer Integration hinzufügen möchten.
8. Wählen Sie Vollständige Konfiguration aus. Nachdem Sie die Konfiguration abgeschlossen haben, können Sie Ihre konfigurierten Integrationen auf der Registerkarte Konfigurierte Integrationen einsehen.

Ein Ticket für eine Integration erstellen ServiceNow ITSM

 Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

Nachdem Sie eine Integration mit erstellt haben ServiceNow ITSM, können Sie ein Ticket für einen Befund erstellen.

 Note

Ein Ergebnis wird während seines gesamten Lebenszyklus immer einem einzelnen Ticket zugeordnet. Alle nachfolgenden Aktualisierungen eines Ergebnisses nach der ersten Erstellung werden an dasselbe Ticket gesendet. Wenn ein mit einer Automatisierungsregel verknüpfter Connector geändert wird, wird der aktualisierte Connector nur für neue und eingehende Ergebnisse verwendet, die den Regelkriterien entsprechen.

Um ein Ticket für einen Befund zu erstellen

1. Melden Sie sich mit Ihren Zugangsdaten bei Ihrem AWS Konto an und öffnen Sie die Security Hub Hub-Konsole unter <https://console.aws.amazon.com/securityhub/v2/home? region=us-ost-1>.

2. Wählen Sie im Navigationsbereich unter Inventar die Option Findings aus.
3. Wählen Sie ein Ergebnis aus. Wählen Sie im Ergebnis die Option Ticket erstellen aus.
4. Öffnen Sie für Integration das Drop-down-Menü und wählen Sie eine Integration aus.
5. Wählen Sie Erstellen aus.

Ein Ticket für eine ServiceNow ITSM Integration anzeigen

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

Nachdem Sie ein Ticket für einen Befund erstellt haben, können Sie das Ticket auf Ihrer ServiceNow ITSM Instanz öffnen.

Um einen Befund auf deiner ServiceNow ITSM Instanz anzusehen

1. Melden Sie sich mit Ihren Zugangsdaten bei Ihrem AWS Konto an und öffnen Sie die Security Hub Hub-Konsole unter <https://console.aws.amazon.com/securityhub/v2/home? region=us-ost-1>.
2. Wählen Sie im Navigationsbereich unter Inventar die Option Findings aus.
3. Wählen Sie die Suche aus, in der Sie das Ticket erstellt haben.
4. Wählen Sie in der Suche die Ticket-ID aus, um das Ticket auf Ihrer ServiceNow ITSM Instanz anzuzeigen, oder wählen Sie „JSON anzeigen“ aus.

Im Übersichts-Dashboard in Security Hub arbeiten

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

In diesem Thema wird das Übersichts-Dashboard in der Security Hub Hub-Konsole beschrieben. Auf dieser Seite finden Sie einen Überblick über Ihre Risiken, Bedrohungen, wichtigsten Ressourcen und den Umfang Ihrer Sicherheitsdienste für mehrere Sicherheits-Widgets. Diese Widgets helfen Ihnen dabei, Sicherheitsrisiken und Bedrohungen nach Schweregrad und Konto nach Sicherheitsfunktionen zu visualisieren. Jedes Mal, wenn Sie diese Seite öffnen, werden die Daten automatisch aktualisiert.

Sie können diese Seite anpassen, indem Sie verschiedene Sicherheits-Widgets hinzufügen und entfernen und Filterkriterien festlegen, um bestimmte Daten in jedem Widget abzurufen. Anpassungen an dieser Seite werden für die future Verwendung gespeichert. Wenn es sich bei Ihrem Konto um das delegierte Administratorkonto für eine Organisation handelt, werden Anpassungen unabhängig von den Anpassungen des Mitgliedskontos gespeichert.

 Note

Wir empfehlen Ihnen, keine vertraulichen, sensiblen oder persönlich identifizierbaren Informationen (PII) in gespeicherte Filter, benutzerdefinierte Widgets oder andere verwandte Freiform-Textfelder aufzunehmen.

Wenn es sich bei Ihrem Konto um das delegierte Administratorkonto für eine Organisation handelt, umfassen die Daten auch Ergebnisse für Ihr Konto und Ihre Mitgliedskonten. Wenn es sich bei Ihrem Konto um ein Mitgliedskonto oder ein eigenständiges Konto handelt, enthalten die Daten nur Ergebnisse für Ihr Konto. Wenn Sie die regionsübergreifende Aggregation in Security Hub konfigurieren, werden auf dieser Seite die Ergebnisse Ihrer Aggregation angezeigt.

Das Widget mit der Zusammenfassung des Risikos

Dieses Widget zeigt alle Ihre Expositionen nach Schweregrad an. Sie können die Häufigkeit jeder Exposition in Ihrer Umgebung sehen. Expositionen mit größerem Schweregrad treten zuerst auf. Die Risiken basieren auf einer Analyse der Ergebnisse und Merkmale von Security Hub und anderen AWS-Services Anbietern wie Amazon Inspector. Die Liste der Risiken in diesem Widget ist auf die acht höchsten Risiken mit der größten Anzahl kritischer Ergebnisse beschränkt. Wenn zwei oder mehr Expositionen die gleiche Anzahl kritischer Ergebnisse aufweisen, werden diese Ergebnisse in der Liste automatisch hinter neueren kritischen Befunden gruppiert.

Das Widget mit der Zusammenfassung der Bedrohungen

Dieses Widget zeigt alle Ihre Bedrohungen nach Schweregrad an. Bedrohungen mit höherem Schweregrad werden zuerst angezeigt. Bedrohungen stehen im Zusammenhang mit einer Reihe von Ereignissen und identifizieren potenzielle Bedrohungen in Ihrer Umgebung. Sie haben auch ihren Ursprung in GuardDuty. Die Liste der Bedrohungen in diesem Widget ist auf die acht Bedrohungen mit dem höchsten Schweregrad beschränkt. Wenn zwei oder mehr Bedrohungen den gleichen Schweregrad haben, gruppiert die Liste diese Ergebnisse automatisch nach neueren Erkenntnissen. Sie müssen GuardDuty die Option aktivieren, um Daten in diesem Widget zu empfangen.

Das Widget „Sicherheitsabdeckung“

Dieses Widget zeigt einen Überblick über Ihren Sicherheitsschutz und basiert auf den Ergebnissen zur Abdeckung der unterstützten Dienste. Es zeigt an, welche Deckungsprüfungen bestanden, fehlgeschlagen sind oder nicht verfügbar sind. Nicht verfügbar bedeutet, dass die Deckungsprüfung nicht abgeschlossen werden kann. Dies kann durch eine gelöschte Ressource oder einen Serverausfall verursacht werden.

Prozentsätze für Deckungsüberprüfungen beziehen sich auf die Anzahl der Prüfungen, die bestanden wurden oder nicht bestanden haben. Beispielsweise ist eine Deckungsprüfung erfolgreich und eine Deckungsprüfung schlägt fehl. Das bedeutet, dass 50% Ihrer Schecks bestanden wurden und 50% Ihrer Schecks nicht bestanden haben. In einigen Fällen werden Prozentsätze auf die nächste ganze Zahl gerundet.

Im Gegensatz zu Sicherheitsdiensten wie GuardDuty Amazon Inspector und Macie veröffentlicht Security Hub CSPM ein Deckungsergebnis pro Konto, das von den aktivierten Standards PASS/FAIL abhängt, z. B. PASS, wenn mindestens ein Standard aktiviert ist. Die Deckungsprozentsätze für Security Hub CSPM sind die Anzahl der Ergebnisse der Security Hub CSPM-Abdeckung, die auf die Gesamtzahl der Ergebnisse der Security Hub CSPM-Abdeckung übergegangen sind.

Note

Wir empfehlen, dass Sie keine vertraulichen, sensiblen oder persönlich identifizierbaren Informationen (PII) in gespeicherte Filter, benutzerdefinierte Widgets oder andere zugehörige Freiform-Textfelder aufnehmen.

Details zu Ressourcen in Security Hub anzeigen

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

Auf der Seite Ressourcen werden allgemeine Ressourcen in Ihrem Konto nachverfolgt. Sie können auf die Seite Ressourcen in der Security Hub Hub-Konsole zugreifen, indem Sie im Navigationsbereich Ressourcen wählen. Wenn Sie einen Ressourcentyp auswählen, können Sie alle

Ressourcen überprüfen, die diesem Ressourcentyp zugeordnet sind. Sie können alle Ergebnisse überprüfen, die mit einer Ressource verknüpft sind.

 Note

Der delegierte Administrator kann alle Ressourcen einsehen, die mit Mitgliedskonten verknüpft sind. Wenn Sie ein Zuhause konfiguriert haben AWS-Region, können Sie alle Ihre Ressourcen in Ihrem Zuhause über AWS-Region AWS-Regionen verlinkt anzeigen.

Wenn Sie eine Ressource auswählen, können Sie die Details zu dieser Ressource überprüfen. Zu diesen Details gehören der Name, die ID, der ARN, der Typ und die Kategorie der Ressource. Sie können die Konto-ID überprüfen, die der Ressource zugeordnet ist, wann die Ressource erstellt wurde (Zeitstempel) und wo die Ressource erstellt wurde (AWS-Region). Sie können auch zusätzliche Details in einem JSON-Snippet überprüfen, das Sie kopieren können.

Wenn Sie von der Registerkarte „Übersicht“ zur Registerkarte „Ergebnisse“ wechseln, können Sie alle mit der Ressource verknüpften Ergebnisse überprüfen. Auf der Registerkarte Ergebnisse werden der Name jedes Ergebnisses, die Art jedes Ergebnisses und der Schweregrad jedes Ergebnisses angezeigt. Sie können Ergebnisse nach verschiedenen Feldern gruppieren und mithilfe von Filtern nach Ergebnissen suchen. Wenn Sie ein Ergebnis auswählen, können Sie sich einen Überblick über das Ergebnis anzeigen lassen, das Informationen zur Einhaltung der Vorschriften und zur Behebung von Problemen im Zusammenhang mit dem Ergebnis enthält. Wenn Sie zu der Ressource zurückkehren, können Sie Ressource öffnen wählen, um die Ressource in der Konsole auf ihren Ressourcentyp zu überprüfen. Wenn es sich bei der Ressource beispielsweise um eine IAM-Ressource handelt, können Sie die Ressource in der IAM-Konsole öffnen.

Die Ressourcenseite bietet Ihnen verschiedene Möglichkeiten, Ressourcen zu organisieren und nach ihnen zu suchen. Sie können Ressourcen nach Typ gruppieren. Sie können Ressourcen beispielsweise nach Konto-ID, Suchtyp, Ressourcenkategorie AWS-Region, Ressourcenname und Ressourcentyp gruppieren. Sie können mithilfe von Filtern nach Ergebnissen suchen. Mithilfe von Schnellfiltern können Sie Ressourcen nach Kategorie, Konten und Suchtypen durchsuchen.

Der Vorteil der Seite Ressourcen besteht darin, dass Sie damit Ihren Sicherheitsstatus überwachen, Ihre Ressourcen organisieren und Details zu Ihren Ressourcen überprüfen können.

Gefährdungen in Security Hub mit dem Diagramm des potenziellen Angriffspfads anzeigen

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

Das Diagramm des potenziellen Angriffspfads ist eine interaktive Visualisierung, die zeigt, wie potenzielle Angreifer auf Ressourcen zugreifen und die Kontrolle darüber übernehmen können, die mit einer Sicherheitslücke verbunden sind. Sie können auf dieses Diagramm nur in der Security Hub Hub-Konsole und über den Bildschirm Exposures zugreifen. Wenn Sie Details zu einem gefundenen Risiko anzeigen, enthält die Registerkarte „Übersicht“ einen Abschnitt mit der Bezeichnung Potenzieller Angriffspfad.

In diesem Abschnitt der Registerkarte „Übersicht“ können Sie AWS Ressourcen auswählen und in das Diagramm mit dem potenziellen Angriffspfad verschieben. Mit den Symbolen zum Vergrößern und Verkleinern können Sie sich auf bestimmte Bereiche des Diagramms mit dem Angriffspfad konzentrieren. Sie können das Diagramm des Angriffspfads im Vollbildmodus und aus dem Vollbildmodus mithilfe des Vollbildsymbols erweitern. Die Legende kennzeichnet die primäre Ressource, die beteiligte Ressource und die Anzahl der beitragenden Eigenschaften farblich und zeigt die Merkmalskategorien und die Anzahl der Eigenschaften im Diagramm des Angriffspfads. Sie können Details zu einer Ressource anzeigen, indem Sie eine Ressource auswählen und dann Ressourcendetails anzeigen wählen. Sie können auch die mit einer Ressource verknüpfte ID und AWS-Konto Nummer kopieren. Offenlegungsergebnisse mit einem Erreichbarkeitsmerkmal zeigen das öffentliche Internet und den zusammengebrochenen Netzwerkpfad im Diagramm des Angriffspfads. Sie können sich dieses Detail ansehen, indem Sie den Knoten mit dem ausgeblendeten Netzwerkpfad auswählen.

Security Hub deaktivieren

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

Wenn Ihr Konto nicht Teil einer Organisation ist, können Sie Security Hub jederzeit in der Security Hub Hub-Konsole deaktivieren. Wenn Sie Security Hub deaktivieren, werden keine Ergebnisse mehr aufgenommen. Außerdem verlieren Sie den Zugriff auf bestehende Ergebnisse und Konfigurationen. Das folgende Verfahren beschreibt, wie Security Hub deaktiviert wird.

Um Security Hub zu deaktivieren

1. Melden Sie sich mit Ihren Zugangsdaten bei Ihrem AWS Konto an und öffnen Sie die Security Hub Hub-Konsole unter <https://console.aws.amazon.com/securityhub/v2/home>.
2. Wählen Sie im Navigationsbereich Allgemein aus.
3. Wählen Sie in Security Hub die Option Deaktivieren aus. Geben Sie im Popup-Fenster Deaktivieren ein und wählen Sie Deaktivieren aus.

Was ist AWS Security Hub CSPM?

AWS Security Hub Cloud Security Posture Management (CSPM) bietet Ihnen einen umfassenden Überblick über Ihren Sicherheitsstatus AWS und hilft Ihnen dabei, Ihre AWS Umgebung anhand von Industriestandards und Best Practices zu bewerten.

Security Hub CSPM sammelt Sicherheitsdaten für und unterstützte Produkte von Drittanbietern und hilft Ihnen dabei AWS-Konten AWS-Services, Ihre Sicherheitstrends zu analysieren und Sicherheitsprobleme mit der höchsten Priorität zu identifizieren.

Um Ihnen bei der Verwaltung des Sicherheitsstatus Ihres Unternehmens zu helfen, unterstützt Security Hub CSPM mehrere Sicherheitsstandards. Dazu gehören der vom Center for Internet Security (CIS) entwickelte AWS Standard AWS Foundational Security Best Practices (FSBP) und externe Compliance-Frameworks wie das Center for Internet Security (CIS), der Payment Card Industry Data Security Standard (PCI DSS) und das National Institute of Standards and Technology (NIST). Jeder Standard umfasst mehrere Sicherheitskontrollen, von denen jede eine bewährte Sicherheitsmethode darstellt. Security Hub CSPM führt Prüfungen anhand von Sicherheitskontrollen durch und generiert Kontrollergebnisse, anhand derer Sie Ihre Einhaltung anhand bewährter Sicherheitsverfahren beurteilen können.

Security Hub CSPM generiert nicht nur Kontrollergebnisse, sondern erhält auch Ergebnisse von anderen Produkten AWS-Services— wie Amazon GuardDuty, Amazon Inspector und Amazon Macie — und von unterstützten Produkten von Drittanbietern. Auf diese Weise haben Sie einen zentralen Überblick über eine Vielzahl von Sicherheitsproblemen. Sie können die Ergebnisse des Security Hub CSPM auch an andere AWS-Services und unterstützte Produkte von Drittanbietern senden.

Security Hub CSPM bietet Automatisierungsfunktionen, mit denen Sie Sicherheitsprobleme erkennen und beheben können. Beispielsweise können Sie Automatisierungsregeln verwenden, um wichtige Ergebnisse automatisch zu aktualisieren, wenn eine Sicherheitsüberprüfung fehlschlägt. Sie können die Integration mit Amazon auch nutzen EventBridge , um automatische Antworten auf bestimmte Ergebnisse auszulösen.

Themen

- [Vorteile von Security Hub CSPM](#)
- [Zugreifen auf Security Hub CSPM](#)
- [Zugehörige Services](#)

- [Kostenlose Testversion von Security Hub CSPM und Preisgestaltung](#)

Vorteile von Security Hub CSPM

Im Folgenden sind einige der wichtigsten Methoden aufgeführt, mit denen Security Hub CSPM Sie bei der Überwachung Ihrer Compliance- und Sicherheitslage in Ihrer AWS gesamten Umgebung unterstützt.

Reduzierter Aufwand zur Erfassung und Priorisierung von Ergebnissen

Security Hub CSPM reduziert den Aufwand für die Erfassung und Priorisierung von Sicherheitsergebnissen für alle Konten aus integrierten Produkten AWS-Services und AWS Partnerprodukten. Security Hub CSPM verarbeitet Suchdaten mit dem AWS Security Finding Format (ASFF), einem Standardsuchformat. Dadurch entfällt die Notwendigkeit, Ergebnisse aus unzähligen Quellen in verschiedenen Formaten zu verwalten. Security Hub CSPM korreliert die Ergebnisse auch anbieterübergreifend, um Ihnen zu helfen, die wichtigsten zu priorisieren.

Automatische Sicherheitsprüfungen nach bewährten Methoden und Standards

Security Hub CSPM führt automatisch kontinuierliche Konfigurationen und Sicherheitsprüfungen auf Kontoebene durch, die auf AWS Best Practices und Industriestandards basieren. Security Hub CSPM verwendet die Ergebnisse dieser Prüfungen, um Sicherheitsbewertungen zu berechnen, und identifiziert bestimmte Konten und Ressourcen, die besondere Aufmerksamkeit erfordern.

Konsolidierte Ansicht der Ergebnisse über Konten und Anbieter hinweg

Security Hub CSPM konsolidiert Ihre Sicherheitsergebnisse für Konten und Anbieterprodukte und zeigt die Ergebnisse auf der Security Hub CSPM-Konsole an. Sie können Ergebnisse auch über die Security Hub CSPM-API, AWS CLI, oder abrufen. SDKs Mit einem ganzheitlichen Überblick über Ihren aktuellen Sicherheitsstatus können Sie Trends erkennen, potenzielle Probleme identifizieren und die erforderlichen Abhilfemaßnahmen ergreifen.

Fähigkeit, die Suche nach Updates und deren Behebung zu automatisieren

Sie können Automatisierungsregeln erstellen, mit denen Ergebnisse auf der Grundlage Ihrer definierten Kriterien geändert oder unterdrückt werden. Security Hub CSPM unterstützt auch eine Integration mit Amazon. EventBridge Um die Behebung bestimmter Ergebnisse zu automatisieren, können Sie benutzerdefinierte Aktionen definieren, die ergriffen werden, wenn ein Ergebnis generiert wird. Sie können beispielsweise benutzerdefinierte Aktionen konfigurieren, damit Ergebnisse an ein Ticketing-System oder ein automatisiertes Behebungssystem gesendet werden.

Zugreifen auf Security Hub CSPM

Security Hub CSPM ist in den meisten Fällen verfügbar. AWS-Regionen Eine Liste der Regionen, in denen Security Hub CSPM derzeit verfügbar ist, finden Sie unter [AWS Security Hub Cloud Security Posture Management \(CSPM\) -Endpunkte](#) und Kontingente in der. Allgemeine AWS-Referenz Informationen zur Verwaltung AWS-Regionen für Sie finden Sie im AWS-Konto Referenzhandbuch unter [Angaben, welche AWS-Regionen Dienste Ihr Konto verwenden kann](#).AWS -Kontenverwaltung

In jeder Region können Sie auf eine der folgenden Arten auf Security Hub CSPM zugreifen und es verwenden:

Security Hub CSPM-Konsole

Das AWS Management Console ist eine browserbasierte Oberfläche, mit der Sie Ressourcen erstellen und verwalten können. AWS Als Teil dieser Konsole bietet die Security Hub CSPM-Konsole Zugriff auf Ihr Security Hub CSPM-Konto, Ihre Daten und Ressourcen. Sie können Security Hub CSPM-Aufgaben mithilfe der Security Hub CSPM-Konsole ausführen — Ergebnisse anzeigen, Automatisierungsregeln erstellen, eine Aggregationsregion erstellen und vieles mehr.

Security Hub CSPM-API

Die Security Hub CSPM-API ermöglicht Ihnen programmatischen Zugriff auf Ihr Security Hub CSPM-Konto, Ihre Daten und Ressourcen. Mit der API können Sie HTTPS-Anfragen direkt an Security Hub CSPM senden. Informationen zur API finden Sie in der [AWS Security Hub Cloud Security Posture Management \(CSPM\) API-Referenz](#).

AWS CLI

Mit dem AWS CLI können Sie Befehle an der Befehlszeile Ihres Systems ausführen, um Security Hub CSPM-Aufgaben auszuführen. In einigen Fällen kann die Verwendung der Befehlszeile schneller und bequemer sein als die Verwendung der Konsole. Die Befehlszeile ist auch nützlich, wenn Sie Skripts erstellen möchten, die Aufgaben ausführen. Informationen zur Installation und Verwendung von finden Sie im [AWS Command Line Interface Benutzerhandbuch](#). AWS CLI

AWS SDKs

AWS SDKs stellt Bibliotheken und Beispielcode für verschiedene Programmiersprachen und Plattformen bereit, z. B. Java, Go, Python, C++ und .NET. SDKs Sie bieten bequemen, programmgesteuerten Zugriff auf Security Hub CSPM und andere Apps AWS-Services in Ihrer bevorzugten Sprache. Sie erledigen auch Aufgaben wie das kryptografische Signieren von Anfragen, das Verwalten von Fehlern und das automatische Wiederholen von Anfragen.

Informationen zur Installation und Verwendung von finden Sie unter [Tools AWS SDKs, auf denen Sie aufbauen können](#). AWS

 Important

Security Hub CSPM erkennt und konsolidiert nur Ergebnisse, die nach der Aktivierung von Security Hub CSPM generiert wurden. Sicherheitsergebnisse, die vor der Aktivierung von Security Hub CSPM generiert wurden, werden nicht rückwirkend erkannt und konsolidiert. Security Hub CSPM empfängt und verarbeitet Ergebnisse nur in der Region, in der Sie Security Hub CSPM in Ihrem Konto aktiviert haben.

Um die vollständige Einhaltung der Benchmark-Sicherheitsprüfungen der CIS AWS Foundations zu gewährleisten, müssen Sie Security Hub CSPM in allen unterstützten AWS Regionen aktivieren.

Zugehörige Services

Um Ihre AWS Umgebung weiter zu schützen, sollten Sie die Verwendung von Other AWS-Services in Kombination mit Security Hub CSPM in Betracht ziehen. Einige AWS-Services senden ihre Ergebnisse an Security Hub CSPM, und Security Hub CSPM normalisiert die Ergebnisse in ein Standardformat. Einige AWS-Services können auch Ergebnisse von Security Hub CSPM erhalten.

Eine Liste anderer Benutzer AWS-Services , die Security Hub CSPM-Ergebnisse senden oder empfangen, finden Sie unter. [AWS-Service Integrationen mit Security Hub CSPM](#)

Security Hub CSPM verwendet dienstbezogene Regeln von, AWS Config um Sicherheitsüberprüfungen für die meisten Kontrollen durchzuführen. Kontrollen beziehen sich auf bestimmte AWS-Services Ressourcen. AWS Eine Liste der Security Hub CSPM-Steuerelemente finden Sie unter. [Kontrollreferenz für Security Hub CSPM](#) Sie müssen Ressourcen AWS Config für Security Hub CSPM aktivieren AWS Config und aufzeichnen, um die meisten Kontrollergebnisse zu generieren. Weitere Informationen finden Sie unter [Überlegungen vor der Aktivierung und Konfiguration AWS Config](#).

Kostenlose Testversion von Security Hub CSPM und Preisgestaltung

Wenn Sie Security Hub CSPM zum ersten Mal aktivieren, wird dieses Konto automatisch AWS-Konto für eine kostenlose 30-Tage-Testversion von Security Hub CSPM registriert.

Wenn Sie Security Hub CSPM während der kostenlosen Testversion verwenden, wird Ihnen die Nutzung anderer Dienste, mit denen Security Hub CSPM interagiert, wie z. B. Artikel, in Rechnung gestellt. AWS Config AWS Config Regeln, die nur durch die Security Hub CSPM-Sicherheitsstandards aktiviert werden, werden Ihnen nicht in Rechnung gestellt.

Die Nutzung von Security Hub CSPM wird Ihnen erst nach Ablauf Ihrer kostenlosen Testversion in Rechnung gestellt.

Anzeigen von Nutzungsdetails und geschätzten Kosten

Security Hub CSPM bietet Nutzungsinformationen, einschließlich der geschätzten 30-Tage-Kosten für die Nutzung von Security Hub CSPM. Die Nutzungsdetails beinhalten die verbleibende Zeit der kostenlosen Testversion. Anhand der Nutzungsinformationen können Sie sich ein Bild davon machen, wie hoch Ihre Security Hub CSPM-Kosten nach Ablauf der kostenlosen Testversion sein könnten. Die Nutzungsinformationen sind auch nach Ablauf der kostenlosen Testversion verfügbar.

Um Nutzungsinformationen anzuzeigen (Konsole)

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Verwendung aus.

Die geschätzten monatlichen Kosten basieren auf der voraussichtlichen Nutzung des Security Hub CSPM durch Ihr Konto für Ergebnisse und Sicherheitschecks über einen Zeitraum von 30 Tagen.

Die Nutzungsinformationen und die geschätzten Kosten beziehen sich nur auf das aktuelle Konto und die aktuelle Region. In einer Aggregationsregion enthalten die Nutzungsinformationen und die geschätzten Kosten keine verknüpften Regionen. Weitere Informationen zu verknüpften Regionen finden Sie unter [the section called “Arten von Daten, die aggregiert sind”](#).

Preisdetails

Weitere Informationen darüber, wie Security Hub CSPM für aufgenommene Ergebnisse und Sicherheitsprüfungen Gebühren erhebt, finden Sie unter [Security Hub](#) CSPM — Preise.

Konzepte und Terminologie in Security Hub CSPM

In AWS Security Hub Cloud Security Posture Management (CSPM) bauen wir auf gemeinsamen AWS Konzepten und Begriffen auf und verwenden diese zusätzlichen Begriffe.

Account

Ein Standardkonto von Amazon Web Services (AWS), das Ihre AWS Ressourcen enthält. Sie können sich AWS mit Ihrem Konto anmelden und Security Hub CSPM aktivieren.

Ein Konto kann andere Konten zur Aktivierung von Security Hub CSPM einladen und mit diesem Konto in Security Hub CSPM verknüpft werden. Das Annehmen einer Mitgliedschaftseinladung ist optional. Wenn die Einladungen angenommen werden, wird das Konto zu einem Administratorkonto und die hinzugefügten Konten sind Mitgliedskonten. Administratorkonten können Ergebnisse in ihren Mitgliedskonten einsehen.

Wenn Sie registriert sind AWS Organizations, weist Ihre Organisation ein Security Hub CSPM-Administratorkonto für die Organisation zu. Das Security Hub CSPM-Administratorkonto kann andere Organisationskonten als Mitgliedskonten aktivieren.

Ein Konto kann nicht gleichzeitig Administratorkonto und Mitgliedskonto sein. Ein Konto kann nur ein Administratorkonto haben.

Weitere Informationen finden Sie unter [Verwaltung von Administrator- und Mitgliedskonten in Security Hub CSPM](#).

Administratorkonto

Ein Konto in Security Hub CSPM, dem Zugriff gewährt wird, um Ergebnisse für zugehörige Mitgliedskonten einzusehen.

Ein Konto wird auf eine der folgenden Arten zu einem Administratorkonto:

- Das Konto lädt andere Konten ein, ihm in Security Hub CSPM zugeordnet zu werden. Wenn diese Konten die Einladung annehmen, werden sie zu Mitgliedskonten und das einladende Konto wird zu ihrem Administratorkonto.
- Das Konto wird von einem Organisationsverwaltungskonto als Security Hub CSPM-Administratorkonto festgelegt. Das Security Hub CSPM-Administratorkonto kann jedes Unternehmenskonto als Mitgliedskonto aktivieren und auch andere Konten als Mitgliedskonten einladen.

Ein Konto kann nur ein Administratorkonto haben. Ein Konto kann nicht gleichzeitig ein Administratorkonto und ein Mitgliedskonto sein.

Aggregationsregion

Wenn Sie eine Aggregationsregion festlegen, können Sie Sicherheitsergebnisse aus mehreren Bereichen AWS-Regionen in einem einzigen Fenster anzeigen.

Die Aggregationsregion ist die Region, von der aus Sie Ergebnisse anzeigen und verwalten. Die Ergebnisse werden aus verknüpften Regionen zur Aggregationsregion aggregiert. Aktualisierungen der Ergebnisse werden in allen Regionen repliziert.

In der Aggregationsregion enthalten die Seiten Sicherheitsstandards, Einblicke und Ergebnisse Daten aus allen verknüpften Regionen.

Weitere Informationen finden Sie unter [Aggregation von CSPM-Daten über Regionen hinweg](#).

Archiviertes Ergebnis

Ein Ergebnis, dessen Datensatzstatus (RecordState) lautet ARCHIVED. Die Archivierung eines Ergebnisses weist darauf hin, dass der Befundgeber der Ansicht ist, dass das Ergebnis nicht mehr relevant ist. Der Datensatzstatus unterscheidet sich vom Workflow-Status, der den Status der Untersuchung bis zu einem Ergebnis verfolgt.

Suchdienstleister können den [BatchImportFindings](#) Betrieb der Security Hub CSPM-API verwenden, um von ihnen erstellte Ergebnisse zu archivieren. Security Hub CSPM archiviert automatisch Kontrollergebnisse, die bestimmte Kriterien erfüllen. Weitere Informationen finden Sie unter [Generierung, Aktualisierung und Archivierung von Kontrollbefunden](#).

Auf der Security Hub CSPM-Konsole schließen die Standardfiltereinstellungen archivierte Ergebnisse aus Suchlisten und Tabellen aus. Sie können die Einstellungen aktualisieren, um archivierte Ergebnisse einzubeziehen. Wenn Sie Ergebnisse mithilfe der [GetFindings](#) Security Hub CSPM-API abrufen, ruft der Vorgang sowohl archivierte als auch aktive Ergebnisse ab. Um archivierte Ergebnisse auszuschließen, können Sie die Ergebnisse filtern. Zum Beispiel:

```
"RecordState": [  
  {  
    "Comparison": "EQUALS",  
    "Value": "ARCHIVED"  
  }  
],
```

AWS Security Finding Format (ASFF)

Ein standardisiertes Format für den Inhalt von Ergebnissen, die Security Hub CSPM aggregiert oder generiert. Mit dem AWS Security Finding Format können Sie Security Hub CSPM verwenden, um Ergebnisse anzuzeigen und zu analysieren, die von AWS Sicherheitsdiensten, Drittanbieterlösungen oder Security Hub CSPM selbst bei der Durchführung von Sicherheitsprüfungen generiert wurden. Weitere Informationen finden Sie unter [AWS Format für Sicherheitssuche \(ASFF\)](#).

Kontrolle

Eine Schutz- oder Gegenmaßnahme, die für ein Informationssystem oder eine Organisation vorgeschrieben ist, um die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationen zu schützen und eine Reihe definierter Sicherheitsanforderungen zu erfüllen. Ein Sicherheitsstandard ist mit einer Sammlung von Kontrollen verknüpft.

Der Begriff Sicherheitskontrolle bezieht sich auf Kontrollen, die standardübergreifend über eine einzige Kontroll-ID und einen einzigen Titel verfügen. Der Begriff Standardkontrolle bezieht sich auf Steuerelemente mit standardspezifischen Steuerelementen IDs und Titeln. Derzeit unterstützt Security Hub CSPM Standardkontrollen nur in den Regionen China und AWS GovCloud (US) Regions Sicherheitskontrollen werden in allen anderen Regionen unterstützt.

Benutzerdefinierte Aktion

Ein Security Hub CSPM-Mechanismus zum Senden ausgewählter Ergebnisse an EventBridge. Eine benutzerdefinierte Aktion wird in Security Hub CSPM erstellt. Sie wird dann mit einer EventBridge Regel verknüpft. Die Regel definiert eine bestimmte Aktion, die ausgeführt werden soll, wenn Funde empfangen werden, die der benutzerdefinierten Aktions-ID zugeordnet sind. Benutzerdefinierte Aktionen können beispielsweise verwendet werden, um einen bestimmten Fund oder einen kleinen Satz von Funden an einen Antwort- oder Korrektur-Workflow zu senden. Weitere Informationen finden Sie unter [the section called “Eine benutzerdefinierte Aktion erstellen”](#).

Delegiertes Administratorkonto (Organizations)

AWS Organizations In kann das delegierte Administratorkonto für einen Dienst die Nutzung eines Dienstes für die Organisation verwalten.

In Security Hub CSPM ist das Security Hub CSPM-Administratorkonto auch das delegierte Administratorkonto für Security Hub CSPM. Wenn das Organisationsverwaltungskonto zum ersten Mal ein Security Hub CSPM-Administratorkonto festlegt, ruft Security Hub CSPM Organizations auf, dieses Konto zum delegierten Administratorkonto zu machen.

Das Organisationsverwaltungskonto muss dann das delegierte Administratorkonto als Security Hub CSPM-Administratorkonto in allen Regionen auswählen.

Erkenntnis

Der beobachtbare Datensatz einer Sicherheitsprüfung oder sicherheitsrelevanten Erkennung. Security Hub CSPM generiert und aktualisiert Ergebnisse, nachdem die Sicherheitsprüfungen für Kontrollen abgeschlossen wurden. Diese Ergebnisse werden als Kontrollergenergebnisse bezeichnet. Die Ergebnisse können auch aus Integrationen mit anderen Produkten AWS-Services und Produkten von Drittanbietern stammen.

Weitere Informationen finden Sie unter [Ergebnisse des CSPM](#).

Regionsübergreifende Aggregation

Die Zusammenfassung von Ergebnissen, Erkenntnissen, Compliance-Status und Sicherheitsbewertungen aus verknüpften Regionen zu einer Aggregationsregion. Anschließend können Sie alle Ihre Daten aus der Aggregationsregion anzeigen und die Ergebnisse und Erkenntnisse aus der Aggregationsregion aktualisieren.

Weitere Informationen finden Sie unter [Aggregation von CSPM-Daten über Regionen hinweg](#).

Erfassung ermitteln

Der Import von Ergebnissen aus anderen AWS Diensten und von Drittanbietern in Security Hub CSPM.

Zu den festgestellten Ingestionseignissen gehören sowohl neue Erkenntnisse als auch Aktualisierungen vorhandener Ergebnisse.

Insight

Eine Sammlung zusammenhängender Funde, die durch eine Aggregationsanweisung und optionale Filter definiert wird. Ein Insight identifiziert einen Sicherheitsbereich, der Aufmerksamkeit und Intervention erfordert. Security Hub CSPM bietet mehrere verwaltete (Standard-) Einblicke, die Sie nicht ändern können. Sie können auch benutzerdefinierte Security Hub CSPM-Einblicke erstellen, um Sicherheitsprobleme zu verfolgen, die für Ihre AWS Umgebung und Nutzung spezifisch sind. Weitere Informationen finden Sie unter [Einblicke in CSPM](#).

Verknüpfte Region

Wenn Sie die regionsübergreifende Aggregation aktivieren, ist eine verknüpfte Region eine Region, die Ergebnisse, Erkenntnisse, den Status der Kontrollkonformität und Sicherheitsbewertungen in der Aggregationsregion zusammenfasst.

In einer verknüpften Region enthalten die Seiten „Ergebnisse“ und „Einblicke“ nur Ergebnisse aus dieser Region.

Weitere Informationen finden Sie unter [Aggregation von CSPM-Daten über Regionen hinweg](#).

Mitgliedskonto

Ein Konto, das einem Administratorkonto die Erlaubnis erteilt hat, die Ergebnisse einzusehen und entsprechende Maßnahmen zu ergreifen.

Ein Konto wird auf eine der folgenden Arten zu einem Mitgliedskonto:

- Das Konto akzeptiert eine Einladung von einem anderen Konto.
- Für ein Organisationskonto aktiviert das Security Hub CSPM-Administratorkonto das Konto als Mitgliedskonto.

Zugehörige Anforderungen

Eine Reihe von Branchen- oder regulatorischen Anforderungen, die einem Steuerelement zugeordnet sind.

Regel

Eine Reihe von automatisierten Kriterien, die verwendet werden, um zu beurteilen, ob ein Steuerelement eingehalten wird. Wenn eine Regel ausgewertet wird, kann sie erfolgreich sein oder fehlschlagen. Wenn die Auswertung nicht feststellen kann, ob die Regel erfolgreich ist oder fehlschlägt, befindet sich die Regel in einem Warnzustand. Wenn die Regel nicht ausgewertet werden kann, befindet sie sich in einem nicht verfügbaren Zustand.

Sicherheitsüberprüfung

Eine spezifische point-in-time Auswertung einer Regel anhand einer einzelnen Ressource, die zu einem Status PASSED, FAILEDWARNING, oder NOT_AVAILABLE führt. Das Ausführen einer Sicherheitsprüfung führt zu einem Ergebnis.

Security Hub CSPM-Administratorkonto

Ein Organisationskonto, das die Security Hub CSPM-Mitgliedschaft für eine Organisation verwaltet.

Das Organisationsverwaltungskonto bestimmt das Security Hub CSPM-Administratorkonto in jeder Region. Das Organisationsverwaltungskonto muss in allen Regionen dasselbe Security Hub CSPM-Administratorkonto wählen.

Das Security Hub CSPM-Administratorkonto ist auch das delegierte Administratorkonto für Security Hub CSPM in Organizations.

Das Security Hub CSPM-Administratorkonto kann jedes Unternehmenskonto als Mitgliedskonto aktivieren. Das Security Hub CSPM-Administratorkonto kann auch andere Konten als Mitgliedskonten einladen.

Sicherheitsstandard

Eine veröffentlichte Erklärung zu einem Thema, in der die Eigenschaften (in der Regel messbar und in Form von Kontrollen) definiert sind, die gegeben sein oder erreicht werden müssen, um Compliance sicherzustellen. Sicherheitsstandards können auf regulatorischen Rahmenbedingungen, bewährten Methoden oder internen Unternehmensrichtlinien basieren. Ein Steuerelement kann mit einem oder mehreren unterstützten Standards in Security Hub CSPM verknüpft sein. Weitere Informationen zu den Sicherheitsstandards in Security Hub CSPM finden Sie unter: [Grundlegendes zu den Sicherheitsstandards in Security Hub CSPM](#)

Schweregrad

Der Schweregrad, der einem Security Hub CSPM-Steuerelement zugewiesen wurde, zeigt die Wichtigkeit der Kontrolle an. Der Schweregrad einer Kontrolle kann „Kritisch“, „Hoch“, „Mittel“, „Niedrig“ oder „Informativ“ sein. Der den Kontrollbefunden zugewiesene Schweregrad entspricht dem Schweregrad der Kontrolle selbst. Informationen darüber, wie Security Hub CSPM einer Kontrolle den Schweregrad zuweist, finden Sie unter: [Schweregrade der Kontrollbefunde](#)

Workflow-Status

Der Status einer Untersuchung zu einem Befund. Dies wird mithilfe des Attributs verfolgt. `Workflow.Status`

Der Workflow-Status ist zunächst NEW. Wenn Sie den Ressourcenbesitzer benachrichtigt haben, Maßnahmen für das Ergebnis zu ergreifen, können Sie den Workflow-Status auf NOTIFIED festlegen. Wenn die Suche kein Problem darstellt und keine Aktion erfordert, legen Sie den Workflow-Status auf SUPPRESSED fest. Nachdem Sie eine Suche überprüft und korrigiert haben, legen Sie den Workflow-Status auf RESOLVED fest.

Standardmäßig enthalten die meisten Suchlisten nur Ergebnisse mit dem Workflow-Status NEW oder NOTIFIED. Die Suche nach Listen für Steuerelemente umfasst auch RESOLVED-Ergebnisse.

Für die Operation [GetFindings](#) können Sie einen Filter für den Workflow-Status einschließen.

```
"WorkflowStatus": [
```

```
{  
  "Comparison": "EQUALS",  
  "Value": "RESOLVED"  
},
```

Die Security Hub CSPM-Konsole bietet eine Option, um den Workflow-Status für Ergebnisse festzulegen. Kunden (oder SIEM-, Ticketing-, Vorfallmanagement- oder SOAR-Tools, die im Auftrag eines Kunden Ergebnisse von Ergebnisanbietern aktualisieren) können mithilfe von [BatchUpdateFindings](#) auch den Workflow-Status aktualisieren.

Security Hub CSPM aktivieren

Es gibt zwei Möglichkeiten, AWS Security Hub Cloud Security Posture Management (CSPM) zu aktivieren: durch Integration mit AWS Organizations oder manuell.

Wir empfehlen dringend die Integration mit Organizations für Umgebungen mit mehreren Konten und mehreren Regionen. Wenn Sie ein eigenständiges Konto haben, müssen Sie Security Hub CSPM manuell einrichten.

Überprüfung der erforderlichen Berechtigungen

Nachdem Sie sich für Amazon Web Services (AWS) angemeldet haben, müssen Sie Security Hub CSPM aktivieren, um dessen Funktionen und Funktionen nutzen zu können. Um Security Hub CSPM zu aktivieren, müssen Sie zunächst Berechtigungen einrichten, die Ihnen den Zugriff auf die Security Hub CSPM-Konsole und API-Operationen ermöglichen. Sie oder Ihr AWS Administrator können dies tun, indem Sie AWS Identity and Access Management (IAM) verwenden, um die AWS verwaltete Richtlinie, die aufgerufen wird `AWSSecurityHubFullAccess`, an Ihre IAM-Identität anzuhängen.

Um Security Hub CSPM über die Organizationsintegration zu aktivieren und zu verwalten, sollten Sie auch die angegebene AWS verwaltete Richtlinie anhängen.
`AWSSecurityHubOrganizationsAccess`

Weitere Informationen finden Sie unter [AWS verwaltete Richtlinien für Security Hub](#).

Aktivierung von Security Hub CSPM mit Unternehmensintegration

Um Security Hub CSPM mit zu verwenden AWS Organizations, bestimmt das AWS Organizations Verwaltungskonto für die Organisation ein Konto als delegiertes Security Hub CSPM-Administratorkonto für die Organisation. Security Hub CSPM wird automatisch im delegierten Administratorkonto in der aktuellen Region aktiviert.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten zur Benennung des delegierten Administrators.

Security Hub CSPM console

So bestimmen Sie beim Onboarding den delegierten Security Hub CSPM-Administrator

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie Gehe zu Security Hub CSPM. Sie werden aufgefordert, sich beim Verwaltungskonto der Organizations anzumelden.
3. Geben Sie auf der Seite Delegierten Administrator benennen im Abschnitt Delegiertes Administratorkonto das delegierte Administratorkonto an. Wir empfehlen, denselben delegierten Administrator zu wählen, den Sie für andere AWS Sicherheits- und Compliance-Dienste eingerichtet haben.
4. Wählen Sie Als delegierten Administrator festlegen aus.

Security Hub CSPM API

Rufen Sie die [EnableOrganizationAdminAccount](#)API über das Verwaltungskonto der Organizations auf. Geben Sie die AWS-Konto ID des delegierten Security Hub-CSPM-Administratorkontos an.

AWS CLI

Führen Sie den [enable-organization-admin-account](#)Befehl über das Verwaltungskonto der Organizations. Geben Sie die AWS-Konto ID des delegierten Security Hub-CSPM-Administratorkontos an.

Beispielbefehl:

```
aws securityhub enable-organization-admin-account --admin-account-id 777788889999
```

Weitere Informationen zur Integration mit Organizations finden Sie unter [Integration von Security Hub CSPM mit AWS Organizations](#).

Zentrale Konfiguration

Wenn Sie Security Hub CSPM und Organizations integrieren, haben Sie die Möglichkeit, eine Funktion namens [zentrale Konfiguration](#) zu verwenden, um Security Hub CSPM für Ihr Unternehmen einzurichten und zu verwalten. Wir empfehlen dringend, die zentrale Konfiguration zu

verwenden, da der Administrator so den Sicherheitsschutz für das Unternehmen anpassen kann. Gegebenenfalls kann der delegierte Administrator einem Mitgliedskonto gestatten, seine eigenen Sicherheitseinstellungen zu konfigurieren.

Die zentrale Konfiguration ermöglicht es dem delegierten Administrator, Security Hub CSPM kontenübergreifend, OUs und zu konfigurieren. AWS-Regionen Der delegierte Administrator konfiguriert Security Hub CSPM, indem er Konfigurationsrichtlinien erstellt. In einer Konfigurationsrichtlinie können Sie die folgenden Einstellungen angeben:

- Ob Security Hub CSPM aktiviert oder deaktiviert ist
- Welche Sicherheitsstandards sind aktiviert und deaktiviert
- Welche Sicherheitskontrollen sind aktiviert und deaktiviert
- Ob Parameter für ausgewählte Steuerelemente angepasst werden sollen

Als delegierter Administrator können Sie eine einzige Konfigurationsrichtlinie für Ihre gesamte Organisation oder verschiedene Konfigurationsrichtlinien für Ihre verschiedenen Konten und OUs erstellen. Beispielsweise können Testkonten und Produktionskonten unterschiedliche Konfigurationsrichtlinien verwenden.

Mitgliedskonten OUs , die eine Konfigurationsrichtlinie verwenden, werden zentral verwaltet und können nur vom delegierten Administrator konfiguriert werden. Der delegierte Administrator kann bestimmte Mitgliedskonten OUs als selbstverwaltete Konten festlegen, sodass das Mitglied seine eigenen Einstellungen auf dieser Grundlage konfigurieren kann. Region-by-Region

Wenn Sie keine zentrale Konfiguration verwenden, müssen Sie Security Hub CSPM für jedes Konto und jede Region weitgehend separat konfigurieren. Dies wird als [lokale](#) Konfiguration bezeichnet. Bei der lokalen Konfiguration kann der delegierte Administrator Security Hub CSPM und eine begrenzte Anzahl von Sicherheitsstandards automatisch in neuen Unternehmenskonten in der aktuellen Region aktivieren. Die lokale Konfiguration gilt nicht für bestehende Organisationskonten oder für andere Regionen als die aktuelle Region. Die lokale Konfiguration unterstützt auch nicht die Verwendung von Konfigurationsrichtlinien.

Manuelles Aktivieren von Security Hub CSPM

Sie müssen Security Hub CSPM manuell aktivieren, wenn Sie ein eigenständiges Konto haben oder wenn Sie es nicht integrieren. AWS Organizations Eigenständige Konten können nicht integriert werden AWS Organizations und müssen manuell aktiviert werden.

Wenn Sie Security Hub CSPM manuell aktivieren, legen Sie ein Security Hub CSPM-Administratorkonto fest und laden andere Konten ein, Mitgliedskonten zu werden. Die Beziehung zwischen Administrator und Mitglied wird hergestellt, wenn ein potenzielles Mitgliedskonto die Einladung annimmt.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um Security Hub CSPM zu aktivieren. Wenn Sie Security Hub CSPM von der Konsole aus aktivieren, haben Sie auch die Möglichkeit, die unterstützten Sicherheitsstandards zu aktivieren.

Security Hub CSPM console

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>
2. Wenn Sie die Security Hub CSPM-Konsole zum ersten Mal öffnen, wählen Sie Gehe zu Security Hub CSPM.
3. Auf der Willkommensseite werden im Abschnitt Sicherheitsstandards die Sicherheitsstandards aufgeführt, die Security Hub CSPM unterstützt.

Aktivieren Sie das Kontrollkästchen für einen Standard, um ihn zu aktivieren, und deaktivieren Sie das Kontrollkästchen, um ihn zu deaktivieren.

Sie können einen Standard oder seine einzelnen Steuerelemente jederzeit aktivieren oder deaktivieren. Informationen zur Verwaltung von Sicherheitsstandards finden Sie unter [Grundlegendes zu den Sicherheitsstandards in Security Hub CSPM](#).

4. Wählen Sie Enable Security Hub (Security Hub aktivieren).

Security Hub CSPM API

Rufen Sie die [EnableSecurityHub](#)API auf. Wenn Sie Security Hub CSPM über die API aktivieren, werden automatisch die folgenden Standardsicherheitsstandards aktiviert:

- AWS Bewährte grundlegende Sicherheitsmethoden
- Benchmark v1.2.0 für die AWS Grundlagen des Zentrums für Internetsicherheit (CIS)

Wenn Sie diese Standards nicht aktivieren möchten, setzen Sie `EnableDefaultStandards` auf `false`.

Sie können den Tags Parameter auch verwenden, um der Hub-Ressource Tag-Werte zuzuweisen.

AWS CLI

Führen Sie den Befehl [enable-security-hub](#) aus. Um die Standardstandards zu aktivieren, schließen Sie ein `--enable-default-standards`. Um die Standardstandards nicht zu aktivieren, fügen Sie hinzu `--no-enable-default-standards`. Die Standardsicherheitsstandards lauten wie folgt:

- AWS Bewährte grundlegende Sicherheitsmethoden
- Benchmark v1.2.0 für die AWS Grundlagen des Zentrums für Internetsicherheit (CIS)

```
aws securityhub enable-security-hub [--tags <tag values>] [--enable-default-standards | --no-enable-default-standards]
```

Beispiel

```
aws securityhub enable-security-hub --enable-default-standards --tags '{"Department": "Security"}
```

Skript zur Aktivierung mehrerer Konten

Note

Anstelle dieses Skripts empfehlen wir, die zentrale Konfiguration zu verwenden, um Security Hub CSPM für mehrere Konten und Regionen zu aktivieren und zu konfigurieren.

Das [Security Hub CSPM-Skript zur Aktivierung mehrerer Konten in GitHub ermöglicht es Ihnen, Security Hub CSPM](#) konto- und regionsübergreifend zu aktivieren. Das Skript automatisiert auch den Prozess des Versendens von Einladungen an Mitgliedskonten und der Aktivierung. AWS Config

Das Skript aktiviert automatisch die AWS Config Ressourcenaufzeichnung für alle Ressourcen, einschließlich globaler Ressourcen, in allen Regionen. Es beschränkt die Aufzeichnung globaler Ressourcen nicht auf eine einzelne Region. Um Kosten zu sparen, empfehlen wir, globale Ressourcen nur in einer einzigen Region zu erfassen. Wenn Sie eine zentrale Konfiguration

oder regionsübergreifende Aggregation verwenden, sollte dies Ihre Heimatregion sein. Weitere Informationen finden Sie unter [Ressourcen aufzeichnen in AWS Config](#).

Es gibt ein entsprechendes Skript, um Security Hub CSPM konto- und regionsübergreifend zu deaktivieren.

Nächste Schritte: Posture-Management und Integrationen

Nach der Aktivierung von Security Hub CSPM empfehlen wir, Sicherheitsstandards und -kontrollen zu aktivieren, um Ihren Sicherheitsstatus zu überwachen. Nachdem Sie die Kontrollen aktiviert haben, beginnt Security Hub CSPM mit der Durchführung von Sicherheitsprüfungen und generiert Kontrollergebnisse, anhand derer Sie Fehlkonfigurationen in Ihrer Umgebung erkennen können. AWS Um Kontrollergebnisse zu erhalten, müssen Sie Security Hub AWS Config CSPM aktivieren und konfigurieren. Weitere Informationen finden Sie unter [Aktivierung und Konfiguration AWS Config für Security Hub CSPM](#).

Nachdem Sie Security Hub CSPM aktiviert haben, können Sie auch Integrationen zwischen Security Hub CSPM und anderen AWS-Services Lösungen und Lösungen von Drittanbietern nutzen, um deren Ergebnisse in Security Hub CSPM zu sehen. Security Hub CSPM aggregiert Ergebnisse aus verschiedenen Quellen und nimmt sie in einem konsistenten Format auf. Weitere Informationen finden Sie unter [Integrationen in Security Hub CSPM verstehen](#).

Aktivierung und Konfiguration AWS Config für Security Hub CSPM

AWS Security Hub Cloud Security Posture Management (CSPM) verwendet AWS Config Regeln, um Sicherheitsprüfungen durchzuführen und Ergebnisse für die meisten Kontrollen zu generieren. AWS Config bietet einen detaillierten Überblick über die Konfiguration der AWS Ressourcen in Ihrem AWS-Konto. Es verwendet Regeln, um eine Basiskonfiguration für Ihre Ressourcen festzulegen, und einen Konfigurationsrekorder, um festzustellen, ob eine bestimmte Ressource gegen die Bedingungen einer Regel verstößt. Einige Regeln, die als AWS Config verwaltete Regeln bezeichnet werden, sind vordefiniert und wurden von AWS Config entwickelt. Andere Regeln sind AWS Config benutzerdefinierte Regeln, die Security Hub CSPM entwickelt.

AWS Config Regeln, die Security Hub CSPM für Kontrollen verwendet, werden als dienstbezogene Regeln bezeichnet. Serviceverknüpfte Regeln ermöglichen es AWS-Services beispielsweise Security Hub CSPM, AWS Config Regeln in Ihrem Konto zu erstellen.

Um Kontrollergebnisse in Security Hub CSPM zu erhalten, müssen Sie die Aktivierung AWS Config in Ihrem Konto aktivieren und die Aufzeichnung für Ressourcen aktivieren, die von Ihnen aktivierten

Kontrollen ausgewertet werden. Auf dieser Seite wird erklärt, wie Sie CSPM AWS Config für Security Hub aktivieren und die Ressourcenaufzeichnung einschalten.

Überlegungen vor der Aktivierung und Konfiguration AWS Config

Um Kontrollergebnisse in Security Hub CSPM zu erhalten, muss Ihr Konto in allen Bereichen AWS Config aktiviert sein, in AWS-Region denen Security Hub CSPM aktiviert ist. Wenn Sie Security Hub CSPM für eine Umgebung mit mehreren Konten verwenden, AWS Config muss es in jeder Region für das Administratorkonto und alle Mitgliedskonten aktiviert sein.

Wir empfehlen dringend, die Ressourcenaufzeichnung zu aktivieren, AWS Config bevor Sie die Security Hub CSPM-Standards und -Steuerelemente aktivieren. Auf diese Weise können Sie sicherstellen, dass Ihre Kontrollergebnisse korrekt sind.

Um die Ressourcenaufzeichnung in zu aktivieren AWS Config, müssen Sie über ausreichende Berechtigungen zum Aufzeichnen von Ressourcen in der AWS Identity and Access Management (IAM) -Rolle verfügen, die dem Konfigurationsrekorder zugeordnet ist. Stellen Sie außerdem sicher, dass keine IAM-Richtlinie oder Richtlinie verwaltet wurde AWS Organizations , die AWS Config verhindert, dass Sie Ihre Ressourcen aufzeichnen dürfen. Security Hub CSPM-Kontrollprüfungen bewerten die Konfiguration einer Ressource direkt und berücksichtigen keine AWS Organizations Richtlinien. Weitere Informationen zur AWS Config Aufzeichnung finden Sie unter [Arbeiten mit dem Konfigurationsrekorder](#) im AWS Config Entwicklerhandbuch.

Wenn Sie einen Standard in Security Hub CSPM aktivieren, ihn aber nicht aktiviert haben AWS Config, versucht Security Hub CSPM, AWS Config Regeln gemäß dem folgenden Zeitplan zu erstellen:

- An dem Tag, an dem Sie den Standard aktivieren.
- Am Tag, nachdem Sie den Standard aktiviert haben.
- 3 Tage, nachdem Sie den Standard aktiviert haben.
- 7 Tage nach der Aktivierung des Standards und danach kontinuierlich alle 7 Tage.

Wenn Sie die zentrale Konfiguration verwenden, versucht Security Hub CSPM jedes Mal, servicebezogene AWS Config Regeln zu erstellen, wenn Sie Konten, Organisationseinheiten (OUs) oder dem Stamm eine Konfigurationsrichtlinie zuordnen, die einen oder mehrere Standards aktiviert.

Ressourcen aufzeichnen in AWS Config

Bei der Aktivierung müssen Sie angeben AWS Config, welche AWS Ressourcen der AWS Config Konfigurationsrekorder aufzeichnen soll. Durch die serviceverknüpften Regeln ermöglicht der Konfigurationsrekorder Security Hub CSPM, Änderungen an Ihren Ressourcenkonfigurationen zu erkennen.

Damit Security Hub CSPM genaue Kontrollergebnisse generiert, müssen Sie die Aufzeichnung AWS Config für die Ressourcen aktivieren, die Ihren aktivierten Kontrollen entsprechen. Es handelt sich in erster Linie um aktivierte Steuerelemente mit einem durch Änderung ausgelösten Zeitplantyp, für den Ressourcen aufgezeichnet werden müssen. Für einige Steuerelemente mit einem periodischen Zeitplan ist auch die Erfassung von Ressourcen erforderlich. Eine Liste dieser Steuerelemente und der entsprechenden Ressourcen finden Sie unter [Erforderliche AWS Config Ressourcen für Kontrollbefunde](#).

Warning

Wenn Sie die AWS Config Aufzeichnung für Security Hub CSPM-Steuerelemente nicht korrekt konfigurieren, kann dies zu ungenauen Kontrollergebnissen führen, insbesondere in den folgenden Fällen:

- Sie haben die Ressource für ein bestimmtes Steuerelement nie aufgezeichnet, oder Sie haben die Aufzeichnung einer Ressource deaktiviert, bevor Sie diesen Ressourcentyp erstellt haben. In diesen Fällen erhalten Sie einen WARNING Befund für das fragliche Steuerelement, obwohl Sie möglicherweise Ressourcen im Bereich des Steuerelements erstellt haben, nachdem Sie die Aufzeichnung deaktiviert haben. Bei diesem WARNING Ergebnis handelt es sich um ein Standardergebnis, bei dem der Konfigurationsstatus der Ressource nicht wirklich bewertet wird.
- Sie deaktivieren die Aufzeichnung für eine Ressource, die von einem bestimmten Steuerelement ausgewertet wird. In diesem Fall behält Security Hub CSPM die Kontrollergebnisse bei, die generiert wurden, bevor Sie die Aufzeichnung deaktiviert haben, obwohl das Steuerelement keine neuen oder aktualisierten Ressourcen auswertet. Security Hub CSPM ändert auch den Compliance-Status der Ergebnisse auf. WARNING Diese gespeicherten Ergebnisse geben möglicherweise nicht genau den aktuellen Konfigurationsstatus einer Ressource wieder.

AWS Config zeichnet standardmäßig alle unterstützten regionalen Ressourcen auf, die es in der Umgebung entdeckt, AWS-Region in der es ausgeführt wird. Um alle Ergebnisse der Security Hub CSPM-Kontrolle zu erhalten, müssen Sie auch die Aufzeichnung globaler AWS Config Ressourcen konfigurieren. Um Kosten zu sparen, empfehlen wir, globale Ressourcen nur in einer einzigen Region zu erfassen. Wenn Sie die zentrale Konfiguration oder die regionsübergreifende Aggregation verwenden, sollte diese Region Ihre Heimatregion sein.

In AWS Config können Sie zwischen kontinuierlicher Aufzeichnung und täglicher Aufzeichnung von Änderungen des Ressourcenstatus wählen. Wenn Sie sich für die tägliche Aufzeichnung AWS Config entscheiden, werden die Ressourcenkonfigurationsdaten am Ende jedes 24-Stunden-Zeitraums bereitgestellt, wenn sich der Ressourcenstatus ändert. Wenn es keine Änderungen gibt, werden keine Daten geliefert. Dies kann die Generierung von Security Hub CSPM-Ergebnissen für durch Änderungen ausgelöste Kontrollen verzögern, bis ein Zeitraum von 24 Stunden abgeschlossen ist.

Weitere Informationen zur AWS Config Aufzeichnung finden Sie im Entwicklerhandbuch unter Ressourcen [aufzeichnen AWS](#).AWS Config

Möglichkeiten zur Aktivierung und Konfiguration AWS Config

Sie können die Ressourcenaufzeichnung auf eine der folgenden Arten aktivieren AWS Config und aktivieren:

- **AWS Config Konsole** — Sie können AWS Config die Aktivierung für ein Konto über die AWS Config Konsole vornehmen. Anweisungen finden Sie im AWS Config Entwicklerhandbuch unter [Einrichtung AWS Config mit der Konsole](#).
- **AWS CLI oder SDKs** — Sie können AWS Config die Aktivierung für ein Konto mithilfe von AWS Command Line Interface (AWS CLI) vornehmen. Eine Anleitung dazu finden Sie unter [Einrichtung AWS Config mit dem AWS CLI](#) im AWS Config Entwicklerhandbuch. AWS Software Development Kits (SDKs) sind auch für viele Programmiersprachen verfügbar.
- **CloudFormation Vorlage** — Zur Aktivierung AWS Config für viele Konten empfehlen wir, die AWS CloudFormation Vorlage mit dem Namen Enable zu verwenden AWS Config. Informationen zum Zugriff auf diese Vorlage finden Sie in den [AWS CloudFormation StackSet Beispielvorlagen](#) im AWS CloudFormation Benutzerhandbuch.

Standardmäßig schließt diese Vorlage Aufzeichnungen für globale IAM-Ressourcen aus. Stellen Sie sicher, dass Sie die Aufzeichnung für globale IAM-Ressourcen nur in einer Version aktivieren, um Aufzeichnungskosten AWS-Region zu sparen. Wenn Sie die regionsübergreifende Aggregation aktiviert haben, sollte dies Ihre [Security Hub CSPM-Heimatregion](#) sein. Andernfalls kann es sich

um jede Region handeln, in der Security Hub CSPM verfügbar ist und die Aufzeichnung globaler IAM-Ressourcen unterstützt. Wir empfehlen, eine StackSet zu starten, um alle Ressourcen, einschließlich globaler IAM-Ressourcen, in der Heimatregion oder einer anderen ausgewählten Region aufzuzeichnen. Führen Sie dann eine Sekunde aus, StackSet um alle Ressourcen außer den globalen IAM-Ressourcen in anderen Regionen aufzuzeichnen.

- **GitHub script** — Security Hub CSPM bietet ein [GitHubSkript](#), das Security Hub CSPM aktiviert, und zwar AWS Config für mehrere Konten in verschiedenen Regionen. Dieses Skript ist nützlich, wenn Sie es nicht integriert haben oder wenn Sie einige Mitgliedskonten haben AWS Organizations, die nicht Teil einer Organisation sind.

Weitere Informationen finden Sie im folgenden Blogbeitrag im AWS Sicherheitsblog: [Optimize AWS Config for AWS Security Hub Cloud Security Posture Management \(CSPM\) zur effektiven Verwaltung Ihres Cloud-Sicherheitsstatus](#).

Config.1-Steuerung

In Security Hub CSPM generiert das [Config.1-Steuerelement](#) FAILED Ergebnisse in Ihrem Konto, wenn AWS Config es deaktiviert ist. Es generiert auch FAILED Ergebnisse in Ihrem Konto, wenn es aktiviert AWS Config ist, aber die Ressourcenaufzeichnung nicht aktiviert ist.

Wenn aktiviert AWS Config ist und die Ressourcenaufzeichnung aktiviert ist, die Ressourcenaufzeichnung jedoch nicht für einen Ressourcentyp aktiviert ist, den ein aktiviertes Steuerelement überprüft, generiert Security Hub CSPM einen FAILED Befund für das Config.1-Steuerelement. Zusätzlich zu diesem FAILED Ergebnis generiert Security Hub CSPM WARNING Ergebnisse für das aktivierte Steuerelement und die Arten von Ressourcen, die das Steuerelement überprüft. Wenn Sie beispielsweise das [KMS.5-Steuerelement](#) aktivieren und die Ressourcenaufzeichnung nicht aktiviert ist AWS KMS keys, generiert Security Hub CSPM einen FAILED Befund für das Config.1-Steuerelement. Security Hub CSPM generiert auch WARNING Ergebnisse für das KMS.5-Steuerelement und Ihre KMS-Schlüssel.

Um ein PASSED Ergebnis für das Config.1-Steuerelement zu erhalten, aktivieren Sie die Ressourcenaufzeichnung für alle Ressourcentypen, die den aktivierten Steuerelementen entsprechen. Deaktivieren Sie außerdem Steuerelemente, die für Ihre Organisation nicht erforderlich sind. Auf diese Weise können Sie sicherstellen, dass Ihre Sicherheitskontrollen keine Konfigurationslücken aufweisen. Auf diese Weise können Sie auch sicherstellen, dass Sie genaue Informationen zu falsch konfigurierten Ressourcen erhalten.

Wenn Sie der delegierte Security Hub CSPM-Administrator für eine Organisation sind, muss die AWS Config Aufzeichnung für Ihr Konto und Ihre Mitgliedskonten korrekt konfiguriert sein. Wenn Sie die regionsübergreifende Aggregation verwenden, muss die AWS Config Aufzeichnung in der Heimatregion und allen verknüpften Regionen korrekt konfiguriert sein. Globale Ressourcen müssen nicht in verknüpften Regionen aufgezeichnet werden.

Generierung der serviceverknüpften Regeln

Für jedes Steuerelement, das eine serviceverknüpfte AWS Config Regel verwendet, erstellt Security Hub CSPM Instanzen der erforderlichen Regel in Ihrer Umgebung. AWS

Diese serviceverknüpften Regeln sind spezifisch für Security Hub CSPM. Security Hub CSPM erstellt diese serviceverknüpften Regeln auch dann, wenn bereits andere Instanzen derselben Regeln existieren. Bei der serviceverknüpften Regel wird `securityhub` vor dem ursprünglichen Regelnamen und nach dem Regelnamen ein eindeutiger Bezeichner hinzugefügt. Für die AWS Config verwaltete Regel `vpc-flow-logs-enabled` könnte der Name der serviceverknüpften Regel beispielsweise lauten: `securityhub-vpc-flow-logs-enabled-12345`

Es gibt Kontingente für die Anzahl der AWS Config verwalteten Regeln, die zur Bewertung von Kontrollen verwendet werden können. AWS Config Regeln, die Security Hub CSPM erstellt, werden nicht auf diese Kontingente angerechnet. Sie können einen Sicherheitsstandard aktivieren, auch wenn Sie das AWS Config Kontingent für verwaltete Regeln in Ihrem Konto bereits erreicht haben. Weitere Informationen zu Kontingenten für AWS Config Regeln finden Sie unter [Dienstbeschränkungen für AWS Config](#) im AWS Config Entwicklerhandbuch.

Kostenüberlegungen

Security Hub CSPM kann sich auf Ihre Kosten für den AWS Config Konfigurationsrekorder auswirken, indem das `AWS::Config::ResourceCompliance` Configurationselement aktualisiert wird. Updates können jedes Mal erfolgen, wenn ein Security Hub CSPM-Steuerelement, das einer AWS Config Regel zugeordnet ist, den Konformitätsstatus ändert, aktiviert oder deaktiviert wird oder Parameter-Updates enthält. Wenn Sie den AWS Config Konfigurationsrekorder nur für Security Hub CSPM verwenden und dieses Configurationselement nicht für andere Zwecke verwenden, empfehlen wir, die Aufzeichnung dafür in zu deaktivieren. AWS Config Dies kann Ihre AWS Config Kosten senken. Sie müssen keine Aufzeichnungen machen, `AWS::Config::ResourceCompliance` damit Sicherheitsüberprüfungen in Security Hub CSPM funktionieren.

[Informationen zu den Kosten im Zusammenhang mit der Ressourcenaufzeichnung finden Sie unter Preise und AWS Config Preise für AWS Security Hub Cloud Security Posture Management \(CSPM\).](#)

Grundlegendes zur lokalen Konfiguration in Security Hub CSPM

Die lokale Konfiguration ist die Standardmethode, mit der eine AWS Organisation in Security Hub CSPM konfiguriert wird. Wenn Sie sich nicht für die zentrale Konfiguration entscheiden und diese aktivieren, verwendet Ihre Organisation standardmäßig die lokale Konfiguration.

Bei der lokalen Konfiguration hat das delegierte Security Hub CSPM-Administratorkonto eingeschränkte Kontrolle über die Konfigurationseinstellungen. Die einzigen Einstellungen, die der delegierte Administrator durchsetzen kann, sind die automatische Aktivierung von Security Hub CSPM und Standardsicherheitsstandards in neuen Unternehmenskonten. Diese Einstellungen gelten nur in der Region, in der Sie das delegierte Administratorkonto angegeben haben. Die Standardsicherheitsstandards sind AWS Foundational Security Best Practices (FSBP) und Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. Lokale Konfigurationseinstellungen gelten nicht für bestehende Organisationskonten oder für andere Regionen als die, für die das delegierte Administratorkonto eingerichtet wurde.

Neben der Aktivierung von Security Hub CSPM und Standardstandards in neuen Organisationskonten in einer einzelnen Region müssen Sie andere Security Hub CSPM-Einstellungen, einschließlich Standards und Kontrollen, für jede Region und jedes Konto separat konfigurieren. Da dies ein doppelter Vorgang sein kann, empfehlen wir, die zentrale Konfiguration für eine Umgebung mit mehreren Konten zu verwenden, wenn eine oder mehrere der folgenden Bedingungen auf Sie zutreffen:

- Sie möchten unterschiedliche Konfigurationseinstellungen für verschiedene Teile Ihrer Organisation (z. B. unterschiedliche aktivierte Standards oder Kontrollen für verschiedene Teams).
- Sie sind in mehreren Regionen tätig und möchten den Zeitaufwand und die Komplexität der Konfiguration des Dienstes in diesen Regionen reduzieren.
- Sie möchten, dass neue Konten bestimmte Konfigurationseinstellungen verwenden, wenn sie der Organisation beitreten.
- Sie möchten, dass Unternehmenskonten bestimmte Konfigurationseinstellungen von einem übergeordneten Konto oder einem Stammkonto erben.

Hinweise zur zentralen Konfiguration finden Sie unter [Grundlegendes zur zentralen Konfiguration in Security Hub CSPM](#).

Grundlegendes zur zentralen Konfiguration in Security Hub CSPM

Die zentrale Konfiguration ist eine AWS Security Hub Cloud Security Posture Management (CSPM) -Funktion, mit der Sie Security Hub CSPM für mehrere und einrichten und verwalten können. AWS-Konten AWS-Regionen Um die zentrale Konfiguration verwenden zu können, müssen Sie zuerst Security Hub CSPM und integrieren. AWS Organizations Sie können die Dienste integrieren, indem Sie eine Organisation erstellen und ein delegiertes Security Hub CSPM-Administratorkonto für die Organisation festlegen.

Über das delegierte Security Hub CSPM-Administratorkonto können Sie Security Hub CSPM für die Konten und Organisationseinheiten () Ihrer Organisation in allen Regionen aktivieren. OUs Sie können auch individuelle Sicherheitsstandards und Sicherheitskontrollen für Konten und regionsübergreifend aktivieren, konfigurieren und deaktivieren. OUs Sie können diese Einstellungen in nur wenigen Schritten von einer Hauptregion aus konfigurieren, die als Heimatregion bezeichnet wird.

Wenn Sie die zentrale Konfiguration verwenden, kann der delegierte Administrator auswählen, welche Konten konfiguriert werden OUs sollen. Wenn der delegierte Administrator ein Mitgliedskonto oder eine Organisationseinheit als selbstverwaltetes Konto festlegt, kann das Mitglied seine eigenen Einstellungen in jeder Region separat konfigurieren. Wenn der delegierte Administrator ein Mitgliedskonto oder eine Organisationseinheit als zentral verwaltet festlegt, kann nur der delegierte Administrator das Mitgliedskonto oder die Organisationseinheit regionsübergreifend konfigurieren. Sie können alle Konten OUs in Ihrer Organisation als zentral verwaltet, alle selbstverwaltet oder als eine Kombination aus beidem festlegen.

Um zentral verwaltete Konten zu konfigurieren, verwendet der delegierte Administrator die Security Hub CSPM-Konfigurationsrichtlinien. Mithilfe von Konfigurationsrichtlinien kann der delegierte Administrator angeben, ob Security Hub CSPM aktiviert oder deaktiviert ist und welche Standards und Kontrollen aktiviert oder deaktiviert sind. Sie können auch verwendet werden, um Parameter für bestimmte Steuerelemente anzupassen.

Konfigurationsrichtlinien werden in der Heimatregion und allen verknüpften Regionen wirksam. Der delegierte Administrator gibt die Heimatregion der Organisation und die verknüpften Regionen an, bevor er die zentrale Konfiguration verwendet. Die Angabe verknüpfter Regionen ist optional. Der delegierte Administrator kann eine einzige Konfigurationsrichtlinie für die gesamte Organisation oder mehrere Konfigurationsrichtlinien erstellen, um variable Einstellungen für verschiedene Konten und OUs zu konfigurieren.

 Tip

Wenn Sie die zentrale Konfiguration nicht verwenden, müssen Sie Security Hub CSPM für jedes Konto und jede Region weitgehend separat konfigurieren. Dies wird als lokale Konfiguration bezeichnet. Bei der lokalen Konfiguration kann der delegierte Administrator Security Hub CSPM und eine begrenzte Anzahl von Sicherheitsstandards automatisch in neuen Unternehmenskonten in der aktuellen Region aktivieren. Die lokale Konfiguration gilt nicht für bestehende Organisationskonten oder für andere Regionen als die aktuelle Region. Die lokale Konfiguration unterstützt auch nicht die Verwendung von Konfigurationsrichtlinien.

Dieser Abschnitt bietet einen Überblick über die zentrale Konfiguration.

Vorteile der Verwendung der zentralen Konfiguration

Die zentrale Konfiguration bietet unter anderem folgende Vorteile:

Vereinfachen Sie die Konfiguration des Security Hub CSPM-Dienstes und der Funktionen

Wenn Sie die zentrale Konfiguration verwenden, führt Sie Security Hub CSPM durch den Prozess der Konfiguration bewährter Sicherheitsmethoden für Ihr Unternehmen. Außerdem werden die daraus resultierenden Konfigurationsrichtlinien automatisch für bestimmte Konten bereitgestellt. OUs Wenn Sie über bestehende Security Hub CSPM-Einstellungen verfügen, z. B. die automatische Aktivierung neuer Sicherheitskontrollen, können Sie diese als Ausgangspunkt für Ihre Konfigurationsrichtlinien verwenden. Darüber hinaus wird auf der Konfigurationsseite der Security Hub CSPM-Konsole in Echtzeit eine Zusammenfassung Ihrer Konfigurationsrichtlinien angezeigt und angegeben, welche Konten und welche Richtlinien OUs verwendet werden.

Konten- und regionsübergreifend konfigurieren

Sie können die zentrale Konfiguration verwenden, um Security Hub CSPM für mehrere Konten und Regionen zu konfigurieren. Auf diese Weise können Sie sicherstellen, dass jeder Teil Ihres Unternehmens eine konsistente Konfiguration und einen angemessenen Sicherheitsschutz beibehält.

Passen Sie unterschiedliche Konfigurationen in unterschiedlichen Konten an und OUs

Bei der zentralen Konfiguration können Sie wählen, ob Sie die Konten Ihrer Organisation auf unterschiedliche OUs Weise konfigurieren möchten. Beispielsweise können für Ihre Testkonten und Produktionskonten unterschiedliche Konfigurationen erforderlich sein. Sie können auch eine Konfigurationsrichtlinie erstellen, die neue Konten abdeckt, wenn diese der Organisation beitreten.

Vermeiden Sie Konfigurationsabweichungen

Konfigurationsabweichungen treten auf, wenn ein Benutzer eine Änderung an einem Dienst oder einer Funktion vornimmt, die mit den Einstellungen des delegierten Administrators in Konflikt steht. Die zentrale Konfiguration verhindert diese Abweichung. Wenn Sie ein Konto oder eine Organisationseinheit als zentral verwaltet kennzeichnen, kann sie nur vom delegierten Administrator der Organisation konfiguriert werden. Wenn Sie es vorziehen, dass ein bestimmtes Konto oder eine bestimmte Organisationseinheit ihre eigenen Einstellungen konfiguriert, können Sie es als selbstverwaltet kennzeichnen.

Wann sollte die zentrale Konfiguration verwendet werden?

Die zentrale Konfiguration ist am vorteilhaftesten für AWS Umgebungen, die mehrere Security Hub CSPM-Konten enthalten. Es wurde entwickelt, um Ihnen zu helfen, Security Hub CSPM für mehrere Konten zentral zu verwalten.

Sie können die zentrale Konfiguration verwenden, um den Security Hub CSPM-Dienst, Sicherheitsstandards und Sicherheitskontrollen zu konfigurieren. Sie können damit auch die Parameter bestimmter Steuerelemente anpassen. Weitere Informationen zu Sicherheitsstandards finden Sie unter [Grundlegendes zu den Sicherheitsstandards in Security Hub CSPM](#). Weitere Informationen zu Sicherheitskontrollen finden Sie unter [Grundlegendes zu den Sicherheitskontrollen in Security Hub CSPM](#).

Zentrale Begriffe und Konzepte zur Konfiguration

Wenn Sie die folgenden wichtigen Begriffe und Konzepte verstehen, können Sie die zentrale Konfiguration von Security Hub CSPM verwenden.

Zentrale Konfiguration

Eine Security Hub CSPM-Funktion, die dem delegierten Security Hub CSPM-Administratorkonto für eine Organisation hilft, den Security Hub CSPM-Dienst, Sicherheitsstandards und Sicherheitskontrollen für mehrere Konten und Regionen zu konfigurieren. Um diese Einstellungen zu konfigurieren, erstellt und verwaltet der delegierte Administrator Security Hub CSPM-Konfigurationsrichtlinien für zentral verwaltete Konten in seiner Organisation. Selbstverwaltete Konten können ihre eigenen Einstellungen in jeder Region separat konfigurieren. Um die zentrale Konfiguration zu verwenden, müssen Sie Security Hub CSPM integrieren. AWS Organizations

Heimatregion

AWS-Region Von dort aus konfiguriert der delegierte Administrator Security Hub CSPM zentral, indem er Konfigurationsrichtlinien erstellt und verwaltet. Konfigurationsrichtlinien gelten in der Heimatregion und allen verknüpften Regionen.

Die Heimatregion dient auch als Security Hub CSPM-Aggregationsregion und empfängt Ergebnisse, Erkenntnisse und andere Daten aus verknüpften Regionen.

Regionen, die am oder nach dem 20. März 2019 AWS eingeführt wurden, werden als Opt-in-Regionen bezeichnet. Eine Opt-in-Region kann nicht die Heimatregion sein, aber es kann sich um eine verknüpfte Region handeln. Eine Liste der Regionen, für die Sie sich anmelden können, finden Sie im Referenzhandbuch zur AWS Kontoverwaltung unter [Überlegungen vor dem Aktivieren und Deaktivieren von Regionen](#).

Verknüpfte Region

Und AWS-Region das kann von der Heimatregion aus konfiguriert werden. Konfigurationsrichtlinien werden vom delegierten Administrator in der Heimatregion erstellt. Die Richtlinien werden in der Heimatregion und allen verknüpften Regionen wirksam. Die Angabe verknüpfter Regionen ist optional.

Eine verknüpfte Region sendet auch Ergebnisse, Erkenntnisse und andere Daten an die Heimatregion.

Regionen, die am oder nach dem 20. März 2019 AWS eingeführt wurden, werden als Opt-in-Regionen bezeichnet. Sie müssen eine solche Region für ein Konto aktivieren, bevor eine Konfigurationsrichtlinie darauf angewendet werden kann. Das Verwaltungskonto für Organizations kann Opt-in-Regionen für ein Mitgliedskonto aktivieren. Weitere Informationen finden [Sie im Referenzhandbuch zur Kontoverwaltung unter Geben Sie an, welche Konten für AWS-Regionen Ihr AWS Konto verwendet werden können](#).

Ziel

Eine AWS-Konto, Organisationseinheit (OU) oder der Organisationsstamm.

Security Hub CSPM-Konfigurationsrichtlinie

Eine Sammlung von Security Hub CSPM-Einstellungen, die der delegierte Administrator für zentral verwaltete Ziele konfigurieren kann. Dies umfasst:

- Ob Security Hub CSPM aktiviert oder deaktiviert werden soll.

- Ob ein oder mehrere [Sicherheitsstandards](#) aktiviert werden sollen.
- Welche [Sicherheitskontrollen](#) für alle aktivierten Standards aktiviert werden sollen. Der delegierte Administrator kann dies tun, indem er eine Liste bestimmter Kontrollen bereitstellt, die aktiviert werden sollten, und Security Hub CSPM deaktiviert alle anderen Kontrollen (einschließlich neuer Kontrollen, wenn sie veröffentlicht werden). Alternativ kann der delegierte Administrator eine Liste bestimmter Kontrollen bereitstellen, die deaktiviert werden sollten, und Security Hub CSPM aktiviert alle anderen Kontrollen (einschließlich neuer Kontrollen, wenn sie veröffentlicht werden).
- [Passen Sie optional die Parameter](#) für ausgewählte aktivierte Steuerelemente in allen aktivierten Standards an.

Eine Konfigurationsrichtlinie wird in der Heimatregion und allen verknüpften Regionen wirksam, nachdem sie mindestens einem Konto, einer Organisationseinheit (OU) oder dem Stammverzeichnis zugeordnet wurde.

Auf der Security Hub CSPM-Konsole kann der delegierte Administrator die von Security Hub CSPM empfohlene Konfigurationsrichtlinie auswählen oder benutzerdefinierte Konfigurationsrichtlinien erstellen. Mit der Security Hub CSPM-API und AWS CLI kann der delegierte Administrator nur benutzerdefinierte Konfigurationsrichtlinien erstellen. Der delegierte Administrator kann maximal 20 benutzerdefinierte Konfigurationsrichtlinien erstellen.

In der empfohlenen Konfigurationsrichtlinie sind Security Hub CSPM, der Standard AWS Foundational Security Best Practices (FSBP) und alle vorhandenen und neuen FSBP-Steuerelemente aktiviert. Steuerelemente, die Parameter akzeptieren, verwenden die Standardwerte. Die empfohlene Konfigurationsrichtlinie gilt für die gesamte Organisation.

Um unterschiedliche Einstellungen auf die Organisation anzuwenden oder unterschiedliche Konfigurationsrichtlinien auf verschiedene Konten anzuwenden und OUs eine benutzerdefinierte Konfigurationsrichtlinie zu erstellen.

Lokale Konfiguration

Der Standardkonfigurationstyp für eine Organisation nach der Integration von Security Hub CSPM und AWS Organizations. Bei der lokalen Konfiguration kann der delegierte Administrator festlegen, dass Security Hub CSPM und [Standardsicherheitsstandards](#) in neuen Unternehmenskonten in der aktuellen Region automatisch aktiviert werden. Wenn der delegierte Administrator automatisch Standardstandards aktiviert, werden alle Kontrollen, die Teil dieser Standards sind, auch automatisch mit Standardparametern für neue Organisationskonten aktiviert. Diese Einstellungen gelten nicht für bestehende Konten, sodass nach dem Beitritt eines Kontos

zur Organisation eine Änderung der Konfiguration möglich ist. Die Deaktivierung bestimmter Kontrollen, die Teil der Standardstandards sind, und die Konfiguration zusätzlicher Standards und Kontrollen müssen für jedes Konto und jede Region separat erfolgen.

Die lokale Konfiguration unterstützt die Verwendung von Konfigurationsrichtlinien nicht. Um Konfigurationsrichtlinien verwenden zu können, müssen Sie zur zentralen Konfiguration wechseln.

Manuelle Kontoverwaltung

Wenn Sie Security Hub CSPM nicht in Security Hub integrieren AWS Organizations oder ein eigenständiges Konto haben, müssen Sie die Einstellungen für jedes Konto in jeder Region separat angeben. Die manuelle Kontoverwaltung unterstützt die Verwendung von Konfigurationsrichtlinien nicht.

Zentrale Konfiguration APIs

Security Hub CSPM-Operationen, die nur der vom Security Hub CSPM delegierte Security Hub CSPM-Administrator in der Heimatregion verwenden kann, um Konfigurationsrichtlinien für zentral verwaltete Konten zu verwalten. Zu den Vorgängen gehören:

- `CreateConfigurationPolicy`
- `DeleteConfigurationPolicy`
- `GetConfigurationPolicy`
- `ListConfigurationPolicies`
- `UpdateConfigurationPolicy`
- `StartConfigurationPolicyAssociation`
- `StartConfigurationPolicyDisassociation`
- `GetConfigurationPolicyAssociation`
- `BatchGetConfigurationPolicyAssociations`
- `ListConfigurationPolicyAssociations`

Kontospezifisch APIs

Security Hub CSPM-Operationen, die verwendet werden können, um Security Hub CSPM, Standards und Kontrollen auf einer bestimmten Basis zu aktivieren oder zu deaktivieren. account-by-account Diese Operationen werden in jeder einzelnen Region verwendet.

Selbstverwaltete Konten können kontospezifische Operationen verwenden, um ihre eigenen Einstellungen zu konfigurieren. Zentral verwaltete Konten können die folgenden kontospezifischen

Vorgänge in der Heimatregion und verknüpften Regionen nicht verwenden. In diesen Regionen kann nur der delegierte Administrator zentral verwaltete Konten über zentrale Konfigurationsvorgänge und Konfigurationsrichtlinien konfigurieren.

- `BatchDisableStandards`
- `BatchEnableStandards`
- `BatchUpdateStandardsControlAssociations`
- `DisableSecurityHub`
- `EnableSecurityHub`
- `UpdateStandardsControl`

Um den Kontostatus zu überprüfen, kann der Besitzer eines zentral verwalteten Kontos `Get` beliebige `Describe` Operationen der Security Hub CSPM-API verwenden.

Wenn Sie statt der zentralen Konfiguration die lokale Konfiguration oder die manuelle Kontoverwaltung verwenden, können Sie diese kontospezifischen Operationen verwenden.

Selbstverwaltete Konten können auch AND-Operationen verwenden `*Invitations`. `*Members` Wir empfehlen jedoch, dass selbstverwaltete Konten diese Operationen nicht verwenden. Richtlinienzuordnungen können fehlschlagen, wenn ein Mitgliedskonto eigene Mitglieder hat, die Teil einer anderen Organisation sind als die des delegierten Administrators.

Organisationseinheit (OU)

In AWS Organizations und Security Hub CSPM, ein Container für eine Gruppe von AWS-Konten Eine Organisationseinheit (OU) kann auch andere enthalten OUs, sodass Sie eine Hierarchie erstellen können, die einem umgedrehten Baum ähnelt, mit einer übergeordneten Organisationseinheit an der Spitze und Verzweigungen OUs dieser Organisationseinheit, die nach unten reichen und in Konten enden, die Blätter des Baums sind. Eine Organisationseinheit kann genau eine übergeordnete Organisationseinheit haben, und jedes Organisationskonto kann Mitglied genau einer Organisationseinheit sein.

Sie können OUs in AWS Organizations oder verwalten AWS Control Tower. Weitere Informationen finden Sie unter [Verwaltung von Organisationseinheiten](#) im AWS Organizations Benutzerhandbuch oder [Verwaltung von Organisationen und Konten mit AWS Control Tower](#) im AWS Control Tower Benutzerhandbuch.

Der delegierte Administrator kann Konfigurationsrichtlinien bestimmten Konten oder dem Stammkonto zuordnen OUs, um alle Konten und OUs innerhalb einer Organisation abzudecken.

Zentral verwaltet

Ein Ziel, das nur der delegierte Administrator mithilfe von Konfigurationsrichtlinien regionsübergreifend konfigurieren kann.

Das delegierte Administratorkonto gibt an, ob ein Ziel zentral verwaltet wird. Der delegierte Administrator kann auch den Status eines Ziels von zentral verwaltet in selbstverwaltet ändern oder umgekehrt.

Selbstverwaltet

Ein Ziel, das seine eigenen Security Hub CSPM-Einstellungen verwaltet. Ein selbstverwaltetes Ziel verwendet kontospezifische Operationen, um Security Hub CSPM für sich selbst in jeder Region separat zu konfigurieren. Dies steht im Gegensatz zu zentral verwalteten Zielen, die nur vom delegierten Administrator regionsübergreifend über Konfigurationsrichtlinien konfiguriert werden können.

Das delegierte Administratorkonto gibt an, ob ein Ziel selbst verwaltet wird. Der delegierte Administrator kann selbstverwaltetes Verhalten auf ein Ziel anwenden. Alternativ kann ein Konto oder eine Organisationseinheit das selbstverwaltete Verhalten von einem Elternteil erben.

Das delegierte Administratorkonto kann selbst ein selbstverwaltetes Konto sein. Das delegierte Administratorkonto kann den Status eines Ziels von selbstverwaltet in zentral verwaltet ändern oder umgekehrt.

Zuordnung von Konfigurationsrichtlinien

Eine Verknüpfung zwischen einer Konfigurationsrichtlinie und einem Konto, einer Organisationseinheit (OU) oder einem Stamm. Wenn eine Richtlinienzuordnung vorhanden ist, verwendet das Konto, die Organisationseinheit oder das Stammverzeichnis die in der Konfigurationsrichtlinie definierten Einstellungen. In einem der folgenden Fälle besteht eine Zuordnung:

- Wenn der delegierte Administrator eine Konfigurationsrichtlinie direkt auf ein Konto, eine Organisationseinheit oder einen Root-Benutzer anwendet
- Wenn ein Konto oder eine Organisationseinheit eine Konfigurationsrichtlinie von einer übergeordneten Organisationseinheit oder der Stammorganisation erbt

Eine Zuordnung besteht, bis eine andere Konfiguration angewendet oder vererbt wird.

Angewendete Konfigurationsrichtlinie

Eine Art von Zuordnung von Konfigurationsrichtlinien, bei der der delegierte Administrator eine Konfigurationsrichtlinie direkt auf Zielkonten oder das Stammkonto anwendet. OUs Ziele werden so konfiguriert, wie sie in der Konfigurationsrichtlinie definiert sind, und nur der delegierte Administrator kann ihre Konfiguration ändern. Wenn die Konfigurationsrichtlinie auf das Stammverzeichnis angewendet wird, wirkt sie sich auf alle Konten und OUs in der Organisation aus, die keine andere Konfiguration verwenden, und zwar entweder durch Anwendung oder Vererbung durch das nächstgelegene übergeordnete Unternehmen.

Der delegierte Administrator kann eine selbstverwaltete Konfiguration auch auf bestimmte Konten oder das OUs Stammkonto anwenden.

Geerbte Konfigurationsrichtlinie

Eine Art von Zuordnung von Konfigurationsrichtlinien, bei der ein Konto oder eine Organisationseinheit die Konfiguration der nächstgelegenen übergeordneten Organisationseinheit oder der Stammorganisation übernimmt. Wenn eine Konfigurationsrichtlinie nicht direkt auf ein Konto oder eine Organisationseinheit angewendet wird, erbt sie die Konfiguration der nächstgelegenen übergeordneten Organisation. Alle Elemente einer Richtlinie werden vererbt. Mit anderen Worten, ein Konto oder eine Organisationseinheit kann sich nicht dafür entscheiden, selektiv nur Teile einer Richtlinie zu erben. Wenn der nächstgelegene Elternteil selbst verwaltet wird, erbt das untergeordnete Konto oder die Organisationseinheit das selbstverwaltete Verhalten des Elternteils.

Die Vererbung kann eine angewendete Konfiguration nicht außer Kraft setzen. Das heißt, wenn eine Konfigurationsrichtlinie oder eine selbstverwaltete Konfiguration direkt auf ein Konto oder eine Organisationseinheit angewendet wird, verwendet sie diese Konfiguration und erbt nicht die Konfiguration der übergeordneten Einheit.

Root

In AWS Organizations und Security Hub CSPM, dem übergeordneten Knoten der obersten Ebene in einer Organisation. Wenn der delegierte Administrator eine Konfigurationsrichtlinie auf Root anwendet, wird die Richtlinie allen Konten und OUs in der Organisation zugeordnet, sofern sie nicht aufgrund von Anwendung oder Vererbung eine andere Richtlinie verwenden oder als selbstverwaltete Benutzerkonten ausgewiesen sind. Wenn der Administrator das Stammverzeichnis als selbstverwaltetes Konto festlegt, werden alle Konten OUs in der Organisation selbst verwaltet, es sei denn, sie verwenden durch Anwendung oder Vererbung eine Konfigurationsrichtlinie. Wenn das Stammkonto selbst verwaltet wird und derzeit keine

Konfigurationsrichtlinien existieren, behalten alle neuen Konten in der Organisation ihre aktuellen Einstellungen bei.

Neue Konten, die einer Organisation beitreten, fallen unter das Stammkonto, bis sie einer bestimmten Organisationseinheit zugewiesen werden. Wenn ein neues Konto keiner Organisationseinheit zugewiesen ist, erbt es die Stammkonfiguration, es sei denn, der delegierte Administrator bestimmt es als selbstverwaltetes Konto.

Aktivierung der zentralen Konfiguration in Security Hub CSPM

Das delegierte AWS Security Hub Cloud Security Posture Management (CSPM) -Administratorkonto kann die zentrale Konfiguration verwenden, um Security Hub CSPM, Standards und Kontrollen für mehrere Konten und Organisationseinheiten () zu konfigurieren. OUs AWS-Regionen

Hintergrundinformationen zu den Vorteilen der zentralen Konfiguration und ihrer Funktionsweise finden Sie unter: [Grundlegendes zur zentralen Konfiguration in Security Hub CSPM](#)

In diesem Abschnitt werden die Voraussetzungen für die zentrale Konfiguration und die ersten Schritte zur Verwendung dieser Konfiguration erläutert.

Voraussetzungen für die zentrale Konfiguration

Bevor Sie die zentrale Konfiguration verwenden können, müssen Sie Security Hub CSPM in die Heimatregion integrieren AWS Organizations und eine Heimatregion festlegen. Wenn Sie die Security Hub CSPM-Konsole verwenden, sind diese Voraussetzungen im Opt-in-Workflow für die zentrale Konfiguration enthalten.

Integrieren Sie mit Organizations

Sie müssen Security Hub CSPM und Organizations integrieren, um die zentrale Konfiguration verwenden zu können.

Um diese Dienste zu integrieren, erstellen Sie zunächst eine Organisation in Organizations. Über das Verwaltungskonto der Organizations bestimmen Sie dann ein delegiertes Security Hub-CSPM-Administratorkonto. Detaillierte Anweisungen finden Sie unter [Integration von Security Hub CSPM mit AWS Organizations](#).

Stellen Sie sicher, dass Sie Ihren delegierten Administrator in Ihrer gewünschten Heimatregion angeben. Wenn Sie die zentrale Konfiguration verwenden, wird derselbe delegierte Administrator

automatisch auch in allen verknüpften Regionen eingerichtet. Das Verwaltungskonto für Organizations kann nicht als delegiertes Administratorkonto festgelegt werden.

 Important

Wenn Sie die zentrale Konfiguration verwenden, können Sie die Security Hub CSPM-Konsole oder Security Hub CSPM nicht verwenden, um das delegierte Administratorkonto APIs zu ändern oder zu entfernen. Wenn das Verwaltungskonto der Organizations verwendet wird AWS Organizations APIs, um den delegierten Security Hub CSPM-Administrator zu ändern oder zu entfernen, stoppt Security Hub CSPM automatisch die zentrale Konfiguration. Ihre Konfigurationsrichtlinien werden ebenfalls getrennt und gelöscht. Mitgliedskonten behalten die Konfiguration bei, die sie hatten, bevor der delegierte Administrator geändert oder entfernt wurde.

Geben Sie eine Heimatregion an

Sie müssen eine Heimatregion angeben, um die zentrale Konfiguration verwenden zu können. Die Heimatregion ist die Region, von der aus der delegierte Administrator die Organisation konfiguriert.

 Note

Bei der Heimatregion kann es sich nicht um eine Region handeln, die als Opt-in-Region ausgewiesen AWS wurde. Eine Opt-in-Region ist standardmäßig deaktiviert. Eine Liste der Opt-in-Regionen finden Sie unter [Überlegungen vor der Aktivierung und Deaktivierung von Regionen im Referenzhandbuch](#) zur AWS Kontoverwaltung.

Optional können Sie eine oder mehrere verknüpfte Regionen angeben, die von der Heimatregion aus konfiguriert werden können.

Der delegierte Administrator kann Konfigurationsrichtlinien nur von der Heimatregion aus erstellen und verwalten. Konfigurationsrichtlinien werden in der Heimatregion und allen verknüpften Regionen wirksam. Sie können keine Konfigurationsrichtlinie erstellen, die nur für eine Teilmenge dieser Regionen gilt und nicht für andere. Eine Ausnahme bilden Steuerungen, die globale Ressourcen betreffen. Wenn Sie die zentrale Konfiguration verwenden, deaktiviert Security Hub CSPM automatisch Kontrollen, die globale Ressourcen in allen Regionen außer der Heimatregion betreffen. Weitere Informationen finden Sie unter [Kontrollen, die globale Ressourcen verwenden](#).

Die Heimatregion ist auch Ihre Security Hub-CSPM-Aggregationsregion, die Ergebnisse, Erkenntnisse und andere Daten aus verknüpften Regionen erhält.

Wenn Sie bereits eine Aggregationsregion für die regionsübergreifende Aggregation festgelegt haben, ist dies Ihre Standard-Heimatregion für die zentrale Konfiguration. Sie können die Heimatregion ändern, bevor Sie die zentrale Konfiguration verwenden, indem Sie Ihren aktuellen Suchaggregator löschen und einen neuen in der gewünschten Heimatregion erstellen. Ein Findingaggregator ist eine Security Hub-CSPM-Ressource, die die Heimatregion und verknüpfte Regionen spezifiziert.

Informationen zur Festlegung einer Heimatregion finden Sie in [den Schritten zum Einstellen](#) einer Aggregationsregion. Wenn Sie bereits eine Heimatregion haben, können Sie die [GetFindingAggregator](#) API aufrufen, um Details zu dieser Region zu sehen, einschließlich der Regionen, die derzeit damit verknüpft sind.

Anweisungen zur Aktivierung der zentralen Konfiguration

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um die zentrale Konfiguration für Ihr Unternehmen zu aktivieren.

Security Hub CSPM console

Um die zentrale Konfiguration (Konsole) zu aktivieren

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Einstellungen und Konfiguration aus. Wählen Sie dann Zentrale Konfiguration starten aus.

Wenn Sie bei Security Hub CSPM einsteigen, wählen Sie Gehe zu Security Hub CSPM.

3. Wählen Sie auf der Seite Delegierten Administrator benennen Ihr delegiertes Administratorkonto aus oder geben Sie dessen Konto-ID ein. Falls zutreffend, empfehlen wir, denselben delegierten Administrator zu wählen, den Sie für andere AWS Sicherheits- und Compliance-Dienste eingerichtet haben. Wählen Sie Als delegierten Administrator festlegen aus.
4. Wählen Sie auf der Seite Organisation zentralisieren im Abschnitt Regionen Ihre Heimatregion aus. Sie müssen in der Heimatregion angemeldet sein, um fortzufahren. Wenn Sie bereits eine Aggregationsregion für die regionsübergreifende Aggregation festgelegt

haben, wird diese als Heimatregion angezeigt. Um die Heimatregion zu ändern, wählen Sie „Regionseinstellungen bearbeiten“. Sie können dann Ihre bevorzugte Heimatregion auswählen und zu diesem Workflow zurückkehren.

5. Wählen Sie mindestens eine Region aus, um eine Verknüpfung mit der Heimatregion herzustellen. Wählen Sie optional aus, ob Sie future unterstützte Regionen automatisch mit der Heimatregion verknüpfen möchten. Die Regionen, die Sie hier auswählen, werden vom delegierten Administrator von der Heimatregion aus konfiguriert. Die Konfigurationsrichtlinien gelten in Ihrer Heimatregion und allen verknüpften Regionen.
6. Wählen Sie Bestätigen und fortfahren.
7. Sie können jetzt die zentrale Konfiguration verwenden. Folgen Sie weiterhin den Anweisungen der Konsole, um Ihre erste Konfigurationsrichtlinie zu erstellen. Wenn Sie noch nicht bereit sind, eine Konfigurationsrichtlinie zu erstellen, wählen Sie Ich bin noch nicht bereit zur Konfiguration. Sie können später eine Richtlinie erstellen, indem Sie im Navigationsbereich Einstellungen und Konfiguration auswählen. Anweisungen zum Erstellen einer Konfigurationsrichtlinie finden Sie unter [Konfigurationsrichtlinien erstellen und zuordnen](#).

Security Hub CSPM API

So aktivieren Sie die zentrale Konfiguration (API)

1. Rufen Sie die [UpdateOrganizationConfiguration](#) API mit den Anmeldeinformationen des delegierten Administratorkontos von der Heimatregion aus auf.
2. Stellen Sie das `AutoEnable` Feld auf ein. `false`
3. Stellen Sie das `ConfigurationType` Feld im `OrganizationConfiguration` Objekt auf ein `CENTRAL`. Diese Aktion hat folgende Auswirkungen:
 - Benennt das anrufende Konto als delegierten Security Hub-CSPM-Administrator in allen verknüpften Regionen.
 - Aktiviert Security Hub CSPM im delegierten Administratorkonto in allen verknüpften Regionen.
 - Benennt das anrufende Konto als delegierten Security Hub CSPM-Administrator für neue und bestehende Konten, die Security Hub CSPM verwenden und zur Organisation gehören. Dies geschieht in der Heimatregion und allen verknüpften Regionen. Das anrufende Konto wird nur dann als delegierter Administrator für neue Organisationskonten eingerichtet, wenn sie einer Konfigurationsrichtlinie zugeordnet sind, für die Security Hub CSPM aktiviert ist. Das anrufende Konto wird nur dann als delegierter Administrator für

bestehende Organisationskonten eingerichtet, wenn Security Hub CSPM bereits aktiviert ist.

- Stellt [AutoEnable](#) auf `false` in allen verknüpften Regionen und [AutoEnableStandards](#) auf `NONE` in der Heimatregion und allen verknüpften Regionen ein. Diese Parameter sind in der Startseite und den verknüpften Regionen nicht relevant, wenn Sie die zentrale Konfiguration verwenden, aber Sie können Security Hub CSPM und Standardsicherheitsstandards in Organisationskonten mithilfe von Konfigurationsrichtlinien automatisch aktivieren.
4. Sie können jetzt die zentrale Konfiguration verwenden. Der delegierte Administrator kann Konfigurationsrichtlinien erstellen, um Security Hub CSPM in Ihrer Organisation zu konfigurieren. Anweisungen zur Erstellung einer Konfigurationsrichtlinie finden Sie unter [Konfigurationsrichtlinien erstellen und zuordnen](#)

Beispiel für eine API-Anfrage:

```
{
  "AutoEnable": false,
  "OrganizationConfiguration": {
    "ConfigurationType": "CENTRAL"
  }
}
```

AWS CLI

Um die zentrale Konfiguration zu aktivieren (AWS CLI)

1. Führen Sie den [update-organization-configuration](#) Befehl mit den Anmeldeinformationen des delegierten Administratorkontos in der Heimatregion aus.
2. Schließen Sie den Parameter `no-auto-enable` ein.
3. Stellen Sie das `ConfigurationType` Feld im `organization-configuration` Objekt auf `CENTRAL` ein. Diese Aktion hat folgende Auswirkungen:
 - Benennt das anrufende Konto als delegierten Security Hub-CSPM-Administrator in allen verknüpften Regionen.
 - Aktiviert Security Hub CSPM im delegierten Administratorkonto in allen verknüpften Regionen.

- Benennt das anrufende Konto als delegierten Security Hub CSPM-Administrator für neue und bestehende Konten, die Security Hub CSPM verwenden und zur Organisation gehören. Dies geschieht in der Heimatregion und allen verknüpften Regionen. Das anrufende Konto wird nur dann als delegierter Administrator für neue Organisationskonten eingerichtet, wenn sie einer Konfigurationsrichtlinie zugeordnet sind, für die Security Hub aktiviert ist. Das anrufende Konto wird nur dann als delegierter Administrator für bestehende Organisationskonten eingerichtet, wenn Security Hub CSPM bereits aktiviert ist.
 - Legt die Option zur automatischen Aktivierung [no-auto-enable](#) in allen verknüpften Regionen und auf NONE in der Heimatregion und allen verknüpften Regionen fest [auto-enable-standards](#). Diese Parameter sind in der Startseite und den verknüpften Regionen nicht relevant, wenn Sie die zentrale Konfiguration verwenden, aber Sie können Security Hub CSPM und Standardsicherheitsstandards in Organisationskonten mithilfe von Konfigurationsrichtlinien automatisch aktivieren.
4. Sie können jetzt die zentrale Konfiguration verwenden. Der delegierte Administrator kann Konfigurationsrichtlinien erstellen, um Security Hub CSPM in Ihrer Organisation zu konfigurieren. Anweisungen zur Erstellung einer Konfigurationsrichtlinie finden Sie unter [Konfigurationsrichtlinien erstellen und zuordnen](#)

Beispielbefehl:

```
aws securityhub --region us-east-1 update-organization-configuration \
--no-auto-enable \
--organization-configuration '{"ConfigurationType": "CENTRAL"}
```

Zentral verwaltete Ziele im Vergleich zu selbstverwalteten Zielen

Wenn Sie die zentrale Konfiguration aktivieren, kann der delegierte AWS Security Hub Cloud Security Posture Management (CSPM) -Administrator jedes Organisationskonto, jede Organisationseinheit (OU) und den Stamm als zentral verwaltet oder selbstverwaltet festlegen. Der Verwaltungstyp eines Ziels bestimmt, wie Sie seine Security Hub CSPM-Einstellungen angeben können.

Hintergrundinformationen zu den Vorteilen der zentralen Konfiguration und ihrer Funktionsweise finden Sie unter [Grundlegendes zur zentralen Konfiguration in Security Hub CSPM](#)

In diesem Abschnitt werden die Unterschiede zwischen einer zentral verwalteten und einer selbstverwalteten Bezeichnung sowie die Auswahl des Verwaltungstyps eines Kontos, einer Organisationseinheit oder eines Stammkontos erläutert.

Selbstverwaltet

Der Besitzer eines selbstverwalteten Kontos, einer Organisationseinheit oder eines Stammkontos muss die Einstellungen für jedes Konto separat konfigurieren. AWS-Region Der delegierte Administrator kann keine Konfigurationsrichtlinien für selbstverwaltete Ziele erstellen.

Zentral verwaltet

Nur der delegierte Security Hub CSPM-Administrator kann Einstellungen für zentral verwaltete Konten oder das Stammkonto in der Heimatregion und den verknüpften Regionen konfigurieren. OUs Konfigurationsrichtlinien können zentral verwalteten Konten und zugeordnet werden. OUs

Der delegierte Administrator kann den Status eines Ziels zwischen selbstverwaltetem und zentral verwaltetem ändern. Standardmäßig werden alle Konten und Organisationseinheiten selbst verwaltet, wenn Sie die zentrale Konfiguration über die Security Hub CSPM-API starten. In der Konsole hängt der Verwaltungstyp von Ihrer ersten Konfigurationsrichtlinie ab. Konten und Konten OUs , die Sie Ihrer ersten Richtlinie zuordnen, werden zentral verwaltet. Andere Konten und OUs werden standardmäßig selbst verwaltet.

Wenn Sie einem zuvor selbstverwalteten Konto eine Konfigurationsrichtlinie zuordnen, haben die Richtlinieneinstellungen Vorrang vor der Bezeichnung für selbstverwaltetes Konto. Das Konto wird zentral verwaltet und übernimmt die Einstellungen, die in der Konfigurationsrichtlinie enthalten sind.

Wenn Sie ein zentral verwaltetes Konto in ein selbstverwaltetes Konto ändern, bleiben die Einstellungen, die zuvor über eine Konfigurationsrichtlinie auf das Konto angewendet wurden, bestehen. Beispielsweise könnte ein zentral verwaltetes Konto zunächst mit einer Richtlinie verknüpft werden, die Security Hub CSPM aktiviert, AWS Foundational Security Best Practices aktiviert und .1 deaktiviert. CloudTrail Wenn Sie das Konto dann als selbstverwaltet kennzeichnen, bleiben alle Einstellungen unverändert. Der Kontoinhaber kann die Einstellungen für das Konto in Zukunft jedoch unabhängig ändern.

Kinderkonten und OUs können selbstverwaltetes Verhalten von einem selbstverwalteten Elternteil erben, genauso wie Kinderkonten und Konfigurationsrichtlinien von einem zentral verwalteten Elternteil erben OUs können. Weitere Informationen finden Sie unter [Richtlinienverknüpfung durch Anwendung und Vererbung](#).

Ein selbstverwaltetes Konto oder eine Organisationseinheit kann keine Konfigurationsrichtlinie von einem übergeordneten Knoten oder vom Stammknoten erben. Wenn Sie beispielsweise möchten, dass alle Konten und OUs in Ihrer Organisation eine Konfigurationsrichtlinie vom Stammverzeichnis erben, müssen Sie den Verwaltungstyp für selbstverwaltete Knoten auf zentral verwaltete Knoten ändern.

Optionen zum Konfigurieren von Einstellungen in selbstverwalteten Konten

Selbstverwaltete Konten müssen ihre eigenen Einstellungen in jeder Region separat konfigurieren.

Besitzer von selbstverwalteten Konten können die folgenden Operationen der Security Hub CSPM-API in jeder Region aufrufen, um ihre Einstellungen zu konfigurieren:

- `EnableSecurityHub` und `DisableSecurityHub` um den Security Hub CSPM-Dienst zu aktivieren oder zu deaktivieren (wenn ein selbstverwaltetes Konto über einen delegierten Security Hub CSPM-Administrator verfügt, muss der Administrator die Kontozuweisung aufheben, bevor [der Kontoinhaber Security Hub CSPM deaktivieren](#) kann).
- `BatchEnableStandards` und `BatchDisableStandards` um Standards zu aktivieren oder zu deaktivieren
- `BatchUpdateStandardsControlAssociations` oder `UpdateStandardsControl` um Steuerungen zu aktivieren oder zu deaktivieren

Selbstverwaltete Konten können auch `*Invitations` `*Members` AND-Operationen verwenden.

Wir empfehlen jedoch, dass selbstverwaltete Konten diese Operationen nicht verwenden.

Richtlinienzuordnungen können fehlschlagen, wenn ein Mitgliedskonto eigene Mitglieder hat, die Teil einer anderen Organisation sind als die des delegierten Administrators.

Eine Beschreibung der Security Hub CSPM-API-Aktionen finden Sie in der [AWS Security Hub Cloud Security Posture Management \(CSPM\)](#) API-Referenz.

Selbstverwaltete Konten können auch die Security Hub CSPM-Konsole verwenden oder AWS CLI ihre Einstellungen in jeder Region konfigurieren.

Selbstverwaltete Konten können keine mit Security Hub APIs zusammenhängenden CSPM-Konfigurationsrichtlinien und Richtlinienzuordnungen aufrufen. Nur der delegierte Administrator kann die zentrale Konfiguration aufrufen APIs und Konfigurationsrichtlinien verwenden, um zentral verwaltete Konten zu konfigurieren.

Auswahl des Verwaltungstyps eines Ziels

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um ein Konto oder eine Organisationseinheit in AWS Security Hub Cloud Security Posture Management (CSPM) als zentral verwaltet oder selbstverwaltet zu kennzeichnen.

Security Hub CSPM console

Um den Verwaltungstyp eines Kontos oder einer Organisationseinheit auszuwählen

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>

Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub CSPM-Administratorkontos in der Heimatregion an.

2. Wählen Sie Konfiguration.
3. Wählen Sie auf der Registerkarte Organisation das Zielkonto oder die Organisationseinheit aus. Wählen Sie Bearbeiten aus.
4. Wählen Sie auf der Seite Konfiguration definieren als Verwaltungstyp die Option Zentral verwaltet aus, wenn der delegierte Administrator das Zielkonto oder die Organisationseinheit konfigurieren soll. Wählen Sie dann „Spezifische Richtlinie anwenden“ aus, wenn Sie dem Ziel eine bestehende Konfigurationsrichtlinie zuordnen möchten. Wählen Sie Von meiner Organisation übernehmen, wenn Sie möchten, dass das Ziel die Konfiguration seines engsten übergeordneten Unternehmens erbt. Wählen Sie Selbstverwaltet, wenn Sie möchten, dass das Konto oder die Organisationseinheit ihre eigenen Einstellungen konfiguriert.
5. Wählen Sie Weiter aus. Überprüfen Sie Ihre Änderungen und wählen Sie Speichern.

Security Hub CSPM API

Um den Verwaltungstyp eines Kontos oder einer Organisationseinheit auszuwählen

1. Rufen Sie die [StartConfigurationPolicyAssociation](#) API über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion auf.
2. Geben Sie für das ConfigurationPolicyIdentifier Feld an, SELF_MANAGED_SECURITY_HUB ob das Konto oder die Organisationseinheit ihre eigenen Einstellungen steuern soll. Geben Sie den Amazon-Ressourcennamen (ARN) oder die ID

der entsprechenden Konfigurationsrichtlinie an, wenn Sie möchten, dass der delegierte Administrator die Einstellungen für das Konto oder die Organisationseinheit steuert.

3. Geben Sie für das Target Feld die AWS-Konto ID, OU-ID oder Root-ID des Ziels ein, dessen Verwaltungstyp Sie ändern möchten. Dadurch wird das selbstverwaltete Verhalten oder die angegebene Konfigurationsrichtlinie dem Ziel zugeordnet. Untergeordnete Konten des Ziels erben möglicherweise die selbstverwaltete Verhaltens- oder Konfigurationsrichtlinie.

Beispiel für eine API-Anfrage zur Benennung eines selbstverwalteten Kontos:

```
{
  "ConfigurationPolicyIdentifier": "SELF_MANAGED_SECURITY_HUB",
  "Target": {"AccountId": "123456789012"}
}
```

AWS CLI

Um den Verwaltungstyp eines Kontos oder einer Organisationseinheit auszuwählen

1. Führen Sie den [start-configuration-policy-association](#) Befehl über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion aus.
2. Geben Sie `configuration-policy-identifizier` im Feld an, `SELF_MANAGED_SECURITY_HUB` ob das Konto oder die Organisationseinheit ihre eigenen Einstellungen steuern soll. Geben Sie den Amazon-Ressourcennamen (ARN) oder die ID der entsprechenden Konfigurationsrichtlinie an, wenn Sie möchten, dass der delegierte Administrator die Einstellungen für das Konto oder die Organisationseinheit steuert.
3. Geben Sie für das `target` Feld die AWS-Konto ID, OU-ID oder Root-ID des Ziels ein, dessen Verwaltungstyp Sie ändern möchten. Dadurch wird das selbstverwaltete Verhalten oder die angegebene Konfigurationsrichtlinie dem Ziel zugeordnet. Untergeordnete Konten des Ziels erben möglicherweise die selbstverwaltete Verhaltens- oder Konfigurationsrichtlinie.

Beispielbefehl zur Benennung eines selbstverwalteten Kontos:

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifizier "SELF_MANAGED_SECURITY_HUB" \
--target '{"AccountId": "123456789012"}'
```

So funktionieren Konfigurationsrichtlinien in Security Hub CSPM

Der delegierte AWS Security Hub Cloud Security Posture Management (CSPM) -Administrator kann Konfigurationsrichtlinien erstellen, um Security Hub CSPM, Sicherheitsstandards und Sicherheitskontrollen für eine Organisation zu konfigurieren. Nach der Erstellung einer Konfigurationsrichtlinie kann der delegierte Administrator sie bestimmten Konten, Organisationseinheiten (OU) oder dem Stamm zuordnen. Die Richtlinie wird dann für die angegebenen Konten oder das Stammkonto wirksam. OUs

Hintergrundinformationen zu den Vorteilen der zentralen Konfiguration und ihrer Funktionsweise finden Sie unter [Grundlegendes zur zentralen Konfiguration in Security Hub CSPM](#).

Dieser Abschnitt bietet einen detaillierten Überblick über die Konfigurationsrichtlinien.

Überlegungen zu Richtlinien

Bevor Sie eine Konfigurationsrichtlinie in Security Hub CSPM erstellen, sollten Sie die folgenden Details berücksichtigen.

- Konfigurationsrichtlinien müssen verknüpft werden, damit sie wirksam werden. Nachdem Sie eine Konfigurationsrichtlinie erstellt haben, können Sie sie einem oder mehreren Konten, Organisationseinheiten (OUs) oder dem Stamm zuordnen. Eine Konfigurationsrichtlinie kann Konten, direkt oder OUs durch Vererbung von einer übergeordneten Organisationseinheit zugeordnet werden.
- Ein Konto oder eine Organisationseinheit kann nur einer Konfigurationsrichtlinie zugeordnet werden. Um widersprüchliche Einstellungen zu vermeiden, kann ein Konto oder eine Organisationseinheit jeweils nur einer Konfigurationsrichtlinie zugeordnet werden. Alternativ kann ein Konto oder eine Organisationseinheit selbst verwaltet werden.
- Die Konfigurationsrichtlinien sind vollständig — Die Konfigurationsrichtlinien bieten eine vollständige Spezifikation der Einstellungen. Beispielsweise kann ein Kinderkonto keine Einstellungen für einige Steuerelemente aus einer Richtlinie und Einstellungen für andere Steuerelemente aus einer anderen Richtlinie akzeptieren. Wenn Sie eine Richtlinie einem Kinderkonto zuordnen, stellen Sie sicher, dass die Richtlinie alle Einstellungen festlegt, die das Kinderkonto verwenden soll.
- Konfigurationsrichtlinien können nicht rückgängig gemacht werden — Es gibt keine Möglichkeit, eine Konfigurationsrichtlinie rückgängig zu machen, nachdem Sie sie Konten oder zugeordnet haben. OUs Wenn Sie beispielsweise eine Konfigurationsrichtlinie, die CloudWatch

Steuerelemente deaktiviert, einem bestimmten Konto zuordnen und diese Richtlinie dann aufheben, sind die CloudWatch Steuerelemente in diesem Konto weiterhin deaktiviert. Um die CloudWatch Kontrollen wieder zu aktivieren, können Sie das Konto einer neuen Richtlinie zuordnen, die die Kontrollen aktiviert. Alternativ können Sie das Konto auf Selbstverwaltung umstellen und alle CloudWatch Steuerelemente im Konto aktivieren.

- Konfigurationsrichtlinien gelten in Ihrer Heimatregion und allen verknüpften Regionen — Eine Konfigurationsrichtlinie wirkt sich auf alle zugehörigen Konten in der Heimatregion und auf alle verknüpften Regionen aus. Sie können keine Konfigurationsrichtlinie erstellen, die nur in einigen dieser Regionen wirksam ist und in anderen nicht. Eine Ausnahme bilden [Steuerelemente, die globale Ressourcen verwenden](#). Security Hub CSPM deaktiviert automatisch Kontrollen, die globale Ressourcen in allen Regionen außer der Heimatregion betreffen.

Regionen, die am oder nach dem 20. März 2019 AWS eingeführt wurden, werden als Opt-in-Regionen bezeichnet. Sie müssen eine solche Region für ein Konto aktivieren, bevor dort eine Konfigurationsrichtlinie wirksam wird. Das Verwaltungskonto für Organizations kann Opt-in-Regionen für ein Mitgliedskonto aktivieren. Anweisungen zur Aktivierung von Opt-in-Regionen finden [Sie im Referenzhandbuch zur Kontoverwaltung unter Geben Sie an, welche Regionen für AWS-Regionen Ihr AWS Konto verwendet werden können](#).

Wenn Ihre Richtlinie eine Steuerung konfiguriert, die in der Heimatregion oder einer oder mehreren verknüpften Regionen nicht verfügbar ist, überspringt Security Hub CSPM die Kontrollkonfiguration in nicht verfügbaren Regionen, wendet die Konfiguration jedoch in Regionen an, in denen die Steuerung verfügbar ist. Ihnen fehlt der Versicherungsschutz für ein Steuerelement, das in der Heimatregion oder einer der verknüpften Regionen nicht verfügbar ist.

- Konfigurationsrichtlinien sind Ressourcen — Als Ressource hat eine Konfigurationsrichtlinie einen Amazon-Ressourcennamen (ARN) und eine Universally Unique Identifier (UUID). Der ARN verwendet das folgende Format: `arn:partition:securityhub:region:delegated administrator account ID:configuration-policy/configuration policy UUID`. Eine selbstverwaltete Konfiguration hat keinen ARN oder UUID. Der Bezeichner für eine selbstverwaltete Konfiguration lautet. SELF_MANAGED_SECURITY_HUB

Arten von Konfigurationsrichtlinien

Jede Konfigurationsrichtlinie legt die folgenden Einstellungen fest:

- Aktivieren oder deaktivieren Sie Security Hub CSPM.
- Aktivieren Sie einen oder mehrere [Sicherheitsstandards](#).

- Geben Sie an, welche [Sicherheitskontrollen](#) für alle aktivierten Standards aktiviert sind. Sie können dies tun, indem Sie eine Liste bestimmter Steuerelemente bereitstellen, die aktiviert werden sollten, und Security Hub CSPM deaktiviert alle anderen Steuerelemente, einschließlich neuer Steuerelemente, wenn sie veröffentlicht werden. Alternativ können Sie eine Liste mit bestimmten Steuerelementen bereitstellen, die deaktiviert werden sollten, und Security Hub CSPM aktiviert alle anderen Kontrollen, einschließlich neuer Steuerelemente, wenn sie veröffentlicht werden.
- [Passen Sie optional die Parameter](#) für ausgewählte aktivierte Steuerelemente für alle aktivierten Standards an.

Zentrale Konfigurationsrichtlinien beinhalten keine AWS Config Rekordereinstellungen. Sie müssen die Aufzeichnung für die erforderlichen Ressourcen separat aktivieren AWS Config und aktivieren, damit Security Hub CSPM Kontrollergebnisse generieren kann. Weitere Informationen finden Sie unter [Überlegungen vor der Aktivierung und Konfiguration AWS Config](#).

Wenn Sie die zentrale Konfiguration verwenden, deaktiviert Security Hub CSPM automatisch Kontrollen, die globale Ressourcen in allen Regionen außer der Heimatregion betreffen. Andere Steuerelemente, die Sie über eine Konfigurationsrichtlinie aktivieren, sind in allen Regionen aktiviert, in denen sie verfügbar sind. Um die Ergebnisse für diese Steuerelemente auf nur eine Region zu beschränken, können Sie Ihre AWS Config Rekordereinstellungen aktualisieren und die globale Ressourcenaufzeichnung in allen Regionen außer der Heimatregion deaktivieren.

Wenn ein aktiviertes Steuerelement, das globale Ressourcen umfasst, in der Heimatregion nicht unterstützt wird, versucht Security Hub CSPM, das Steuerelement in einer verknüpften Region zu aktivieren, in der das Steuerelement unterstützt wird. Bei zentraler Konfiguration fehlt Ihnen die Abdeckung für ein Steuerelement, das in der Heimatregion oder einer der verknüpften Regionen nicht verfügbar ist.

Eine Liste der Steuerelemente, die globale Ressourcen betreffen, finden Sie unter [Kontrollen, die globale Ressourcen verwenden](#).

Empfohlene Konfigurationsrichtlinie

Wenn Sie zum ersten Mal eine Konfigurationsrichtlinie in der Security Hub CSPM-Konsole erstellen, haben Sie die Möglichkeit, die von Security Hub CSPM empfohlene Richtlinie auszuwählen.

Die empfohlene Richtlinie aktiviert Security Hub CSPM, den Standard AWS Foundational Security Best Practices (FSBP) und alle vorhandenen und neuen FSBP-Steuerelemente. Steuerelemente, die Parameter akzeptieren, verwenden die Standardwerte. Die empfohlene Richtlinie gilt für Root-

Benutzer (alle Konten und OUs sowohl neue als auch bestehende). Nachdem Sie die empfohlene Richtlinie für Ihre Organisation erstellt haben, können Sie sie über das delegierte Administratorkonto ändern. Sie können beispielsweise zusätzliche Standards oder Kontrollen aktivieren oder bestimmte FSBP-Steuerelemente deaktivieren. Anweisungen zum Ändern einer Konfigurationsrichtlinie finden Sie unter [Aktualisierung der Konfigurationsrichtlinien](#).

Benutzerdefinierte Konfigurationsrichtlinie

Anstelle der empfohlenen Richtlinie kann der delegierte Administrator bis zu 20 benutzerdefinierte Konfigurationsrichtlinien erstellen. Sie können Ihrer gesamten Organisation eine einzelne benutzerdefinierte Richtlinie oder verschiedene benutzerdefinierte Richtlinien verschiedenen Konten zuordnen und OUs. Für eine benutzerdefinierte Konfigurationsrichtlinie geben Sie Ihre gewünschten Einstellungen an. Sie können beispielsweise eine benutzerdefinierte Richtlinie erstellen, die FSBP, den Center for Internet Security (CIS) AWS Foundations Benchmark v1.4.0 und alle Kontrollen in diesen Standards außer Amazon Redshift Redshift-Steuerelementen aktiviert. Die Granularität, die Sie in benutzerdefinierten Konfigurationsrichtlinien verwenden, hängt vom beabsichtigten Umfang der Sicherheitsabdeckung in Ihrem Unternehmen ab.

Note

Sie können dem delegierten Administratorkonto keine Konfigurationsrichtlinie zuordnen, die Security Hub CSPM deaktiviert. Eine solche Richtlinie kann mit anderen Konten verknüpft werden, überspringt jedoch die Zuordnung zum delegierten Administrator. Das delegierte Administratorkonto behält seine aktuelle Konfiguration bei.

Nachdem Sie eine benutzerdefinierte Konfigurationsrichtlinie erstellt haben, können Sie zur empfohlenen Konfigurationsrichtlinie wechseln, indem Sie Ihre Konfigurationsrichtlinie entsprechend der empfohlenen Konfiguration aktualisieren. Sie sehen jedoch nicht die Möglichkeit, die empfohlene Konfigurationsrichtlinie in der Security Hub CSPM-Konsole zu erstellen, nachdem Ihre erste Richtlinie erstellt wurde.

Richtlinienverknüpfung durch Anwendung und Vererbung

Wenn Sie sich zum ersten Mal für die zentrale Konfiguration entscheiden, hat Ihre Organisation keine Zuordnungen und verhält sich genauso wie vor der Anmeldung. Der delegierte Administrator kann dann Verknüpfungen zwischen einer Konfigurationsrichtlinie oder einem selbstverwalteten Verhalten und Konten oder dem Stammkonto herstellen. OUs Verknüpfungen können durch Anwendung oder Vererbung hergestellt werden.

Über das delegierte Administratorkonto können Sie eine Konfigurationsrichtlinie direkt auf ein Konto, eine Organisationseinheit oder das Stammkonto anwenden. Alternativ kann der delegierte Administrator einem Konto, einer Organisationseinheit oder dem Stammkonto direkt eine selbstverwaltete Bezeichnung zuweisen.

In Ermangelung einer direkten Anwendung erbt ein Konto oder eine Organisationseinheit die Einstellungen der nächstgelegenen übergeordneten Organisation, die über eine Konfigurationsrichtlinie oder ein selbstverwaltetes Verhalten verfügt. Wenn das engste Elternteil mit einer Konfigurationsrichtlinie verknüpft ist, erbt das Kind diese Richtlinie und kann nur vom delegierten Administrator aus der Heimatregion konfiguriert werden. Wenn der nächstgelegene Elternteil selbst verwaltet wird, erbt das Kind das selbstverwaltete Verhalten und kann in jedem Fall seine eigenen Einstellungen angeben. AWS-Region

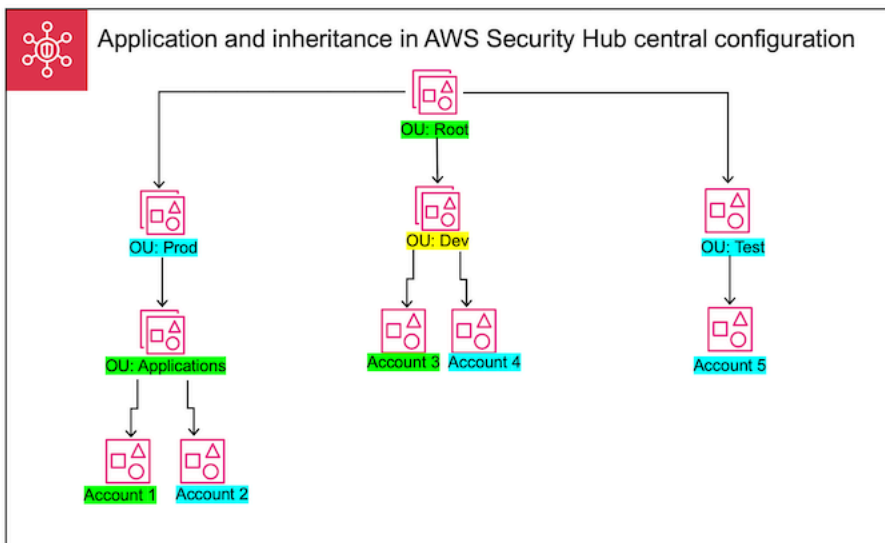
Die Anwendung hat Vorrang vor der Vererbung. Mit anderen Worten, die Vererbung setzt eine Konfigurationsrichtlinie oder eine selbstverwaltete Bestimmung, die der delegierte Administrator direkt auf ein Konto oder eine Organisationseinheit angewendet hat, nicht außer Kraft.

Wenn Sie eine Konfigurationsrichtlinie direkt auf ein selbstverwaltetes Konto anwenden, hat die Richtlinie Vorrang vor der Bezeichnung für selbstverwaltete Konten. Das Konto wird zentral verwaltet und übernimmt die Einstellungen, die in der Konfigurationsrichtlinie enthalten sind.

Wir empfehlen, eine Konfigurationsrichtlinie direkt auf das Stammverzeichnis anzuwenden. Wenn Sie eine Richtlinie auf das Stammverzeichnis anwenden, erben neue Konten, die Ihrer Organisation beitreten, automatisch die Stammrichtlinie, sofern Sie sie nicht einer anderen Richtlinie zuordnen oder sie als selbstverwaltet kennzeichnen.

Einem Konto oder einer Organisationseinheit kann jeweils nur eine Konfigurationsrichtlinie zugeordnet werden, entweder durch Anwendung oder Vererbung. Dadurch sollen widersprüchliche Einstellungen vermieden werden.

Das folgende Diagramm zeigt, wie die Anwendung und Vererbung von Richtlinien in einer zentralen Konfiguration funktionieren.



In diesem Beispiel wurde auf einen grün hervorgehobenen Knoten eine Konfigurationsrichtlinie angewendet. Auf einen blau hervorgehobenen Knoten wurde keine Konfigurationsrichtlinie angewendet. Ein gelb hervorgehobener Knoten wurde als selbstverwaltet eingestuft. Jedes Konto und jede Organisationseinheit verwendet die folgende Konfiguration:

- OU:Root (Grün) — Diese Organisationseinheit verwendet die Konfigurationsrichtlinie, die auf sie angewendet wurde.
- ou:Prod (Blue) — Diese OU erbt die Konfigurationsrichtlinie von OU:Root.
- ou:Applications (Green) — Diese Organisationseinheit verwendet die Konfigurationsrichtlinie, die auf sie angewendet wurde.
- Konto 1 (Grün) — Dieses Konto verwendet die Konfigurationsrichtlinie, die darauf angewendet wurde.
- Konto 2 (Blau) — Dieses Konto erbt die Konfigurationsrichtlinie von OU:Applications.
- ou:Dev (Gelb) — Diese Organisationseinheit wird selbst verwaltet.
- Konto 3 (Grün) — Dieses Konto verwendet die Konfigurationsrichtlinie, die darauf angewendet wurde.
- Konto 4 (Blau) — Dieses Konto erbt das selbstverwaltete Verhalten von OU:Dev.
- ou:Test (Blue) — Dieses Konto erbt die Konfigurationsrichtlinie von ou:Root.
- Konto 5 (Blau) — Dieses Konto erbt die Konfigurationsrichtlinie von ou:Root, da das unmittelbar übergeordnete Konto, ou:Test, keiner Konfigurationsrichtlinie zugeordnet ist.

Testen einer Konfigurationsrichtlinie

Um sicherzustellen, dass Sie verstehen, wie Konfigurationsrichtlinien funktionieren, empfehlen wir, eine Richtlinie zu erstellen und sie einem Testkonto oder einer Organisationseinheit zuzuordnen.

Um eine Konfigurationsrichtlinie zu testen

1. Erstellen Sie eine benutzerdefinierte Konfigurationsrichtlinie und stellen Sie sicher, dass die angegebenen Einstellungen für die Aktivierung, Standards und Kontrollen von Security Hub CSPM korrekt sind. Detaillierte Anweisungen finden Sie unter [Konfigurationsrichtlinien erstellen und zuordnen](#).
2. Wenden Sie die Konfigurationsrichtlinie auf ein Testkonto oder eine Organisationseinheit an, die keine Kinderkonten hat oder OUs
3. Stellen Sie sicher, dass das Testkonto oder die Organisationseinheit die Konfigurationsrichtlinie in Ihrer Heimatregion und allen verknüpften Regionen erwartungsgemäß verwendet. Sie können auch überprüfen, ob alle anderen Konten und OUs in Ihrer Organisation weiterhin selbst verwaltet werden, und Sie können ihre eigenen Einstellungen in jeder Region ändern.

Nachdem Sie eine Konfigurationsrichtlinie in einem einzelnen Konto oder einer Organisationseinheit getestet haben, können Sie sie anderen Konten zuordnen und OUs.

Konfigurationsrichtlinien erstellen und zuordnen

Das delegierte AWS Security Hub Cloud Security Posture Management (CSPM) -Administratorkonto kann Konfigurationsrichtlinien erstellen, die festlegen, wie Security Hub CSPM, Standards und Kontrollen in bestimmten Konten und Organisationseinheiten konfiguriert werden (). OUs Eine Konfigurationsrichtlinie wird erst wirksam, wenn der delegierte Administrator sie mindestens einem Konto oder einer Organisationseinheit () OUs oder dem Stamm zuordnet. Der delegierte Administrator kann eine selbstverwaltete Konfiguration auch Konten oder dem Stammverzeichnis OUs zuordnen.

Wenn Sie zum ersten Mal eine Konfigurationsrichtlinie erstellen, empfehlen wir, diese zuerst zu überprüfen. [So funktionieren Konfigurationsrichtlinien in Security Hub CSPM](#)

Wählen Sie Ihre bevorzugte Zugriffsmethode und folgen Sie den Schritten zum Erstellen und Zuordnen einer Konfigurationsrichtlinie oder einer selbstverwalteten Konfiguration. Wenn Sie die Security Hub CSPM-Konsole verwenden, können Sie eine Konfiguration mehreren Konten oder OUs

gleichzeitig zuordnen. Wenn Sie die Security Hub CSPM API oder verwenden AWS CLI, können Sie in jeder Anfrage nur einem Konto oder einer Organisationseinheit eine Konfiguration zuordnen.

 Note

Wenn Sie die zentrale Konfiguration verwenden, deaktiviert Security Hub CSPM automatisch Kontrollen, die globale Ressourcen in allen Regionen außer der Heimatregion betreffen. Andere Steuerelemente, die Sie über eine Konfigurationsrichtlinie aktivieren, sind in allen Regionen aktiviert, in denen sie verfügbar sind. Um die Ergebnisse für diese Steuerelemente auf nur eine Region zu beschränken, können Sie Ihre AWS Config Rekordereinstellungen aktualisieren und die globale Ressourcenaufzeichnung in allen Regionen außer der Heimatregion deaktivieren.

Wenn ein aktiviertes Steuerelement, das globale Ressourcen umfasst, in der Heimatregion nicht unterstützt wird, versucht Security Hub CSPM, das Steuerelement in einer verknüpften Region zu aktivieren, in der das Steuerelement unterstützt wird. Bei zentraler Konfiguration fehlt Ihnen die Abdeckung für ein Steuerelement, das in der Heimatregion oder einer der verknüpften Regionen nicht verfügbar ist.

Eine Liste der Steuerelemente, die globale Ressourcen betreffen, finden Sie unter [Kontrollen, die globale Ressourcen verwenden](#).

Security Hub CSPM console

So erstellen Sie Konfigurationsrichtlinien und ordnen sie zu

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>

Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub CSPM-Administratorkontos in der Heimatregion an.

2. Wählen Sie im Navigationsbereich Konfiguration und dann die Registerkarte Richtlinien aus. Wählen Sie dann Richtlinie erstellen aus.
3. Wenn Sie zum ersten Mal eine Konfigurationsrichtlinie erstellen, werden auf der Seite Organisation konfigurieren unter Konfigurationstyp drei Optionen angezeigt. Wenn Sie bereits mindestens eine Konfigurationsrichtlinie erstellt haben, wird nur die Option Benutzerdefinierte Richtlinie angezeigt.

- Wählen Sie Die AWS empfohlene Security Hub CSPM-Konfiguration für mein gesamtes Unternehmen verwenden, um unsere empfohlene Richtlinie zu verwenden. Die empfohlene Richtlinie aktiviert Security Hub CSPM in allen Unternehmenskonten, aktiviert den Standard AWS Foundational Security Best Practices (FSBP) und aktiviert alle neuen und vorhandenen FSBP-Steuerelemente. Die Steuerelemente verwenden Standardparameterwerte.
 - Wählen Sie Ich bin noch nicht bereit zur Konfiguration, um später eine Konfigurationsrichtlinie zu erstellen.
 - Wählen Sie Benutzerdefinierte Richtlinie, um eine benutzerdefinierte Konfigurationsrichtlinie zu erstellen. Geben Sie an, ob Security Hub CSPM aktiviert oder deaktiviert werden soll, welche Standards aktiviert werden sollen und welche Kontrollen für diese Standards aktiviert werden sollen. Geben Sie optional [benutzerdefinierte Parameterwerte](#) für ein oder mehrere aktivierte Steuerelemente an, die benutzerdefinierte Parameter unterstützen.
4. Wählen Sie im Abschnitt Konten die Zielkonten oder das Stammkonto aus, OUs für das Ihre Konfigurationsrichtlinie gelten soll.
- Wählen Sie Alle Konten aus, wenn Sie die Konfigurationsrichtlinie auf das Stammkonto anwenden möchten. Dies schließt alle Konten und Konten OUs in der Organisation ein, auf die keine andere Richtlinie angewendet oder vererbt wurde.
 - Wählen Sie Bestimmte Konten aus, wenn Sie die Konfigurationsrichtlinie auf bestimmte Konten anwenden möchten oder OUs. Geben Sie das Konto ein IDs, oder wählen Sie die Konten und OUs aus der Organisationsstruktur aus. Sie können die Richtlinie bei der Erstellung auf maximal 15 Ziele (Konten oder Root) anwenden. OUs Wenn Sie eine größere Anzahl angeben möchten, bearbeiten Sie Ihre Richtlinie nach der Erstellung und wenden Sie sie auf weitere Ziele an.
 - Wählen Sie Nur der delegierte Administrator, um die Konfigurationsrichtlinie auf das aktuelle delegierte Administratorkonto anzuwenden.
5. Wählen Sie Weiter aus.
6. Überprüfen Sie auf der Seite Überprüfen und Anwenden die Details Ihrer Konfigurationsrichtlinie. Wählen Sie dann Richtlinie erstellen und anwenden aus. In Ihrer Heimatregion und den verknüpften Regionen setzt diese Aktion die vorhandenen Konfigurationseinstellungen der Konten außer Kraft, die dieser Konfigurationsrichtlinie zugeordnet sind. Konten können über eine Anwendung oder durch Vererbung von einem übergeordneten Knoten mit der Konfigurationsrichtlinie verknüpft werden. Untergeordnete

Konten und OUs die angewendeten Ziele erben automatisch diese Konfigurationsrichtlinie, sofern sie nicht ausdrücklich ausgeschlossen wurden, sie selbst verwaltet werden oder eine andere Konfigurationsrichtlinie verwenden.

Security Hub CSPM API

Um Konfigurationsrichtlinien zu erstellen und zuzuordnen

1. Rufen Sie die [CreateConfigurationPolicy](#) API über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion auf.
2. Geben Sie für Name einen eindeutigen Namen für die Konfigurationsrichtlinie ein. Geben Sie optional für Description eine Beschreibung der Konfigurationsrichtlinie an.
3. Geben Sie für das ServiceEnabled Feld an, ob Security Hub CSPM in dieser Konfigurationsrichtlinie aktiviert oder deaktiviert werden soll.
4. Geben Sie für das EnabledStandardIdentifiers Feld an, welche Security Hub CSPM-Standards Sie in dieser Konfigurationsrichtlinie aktivieren möchten.
5. Geben Sie für das SecurityControlsConfiguration Objekt an, welche Steuerelemente Sie in dieser Konfigurationsrichtlinie aktivieren oder deaktivieren möchten. Wählen Sie EnabledSecurityControlIdentifiers aus, dass die angegebenen Steuerelemente aktiviert sind. Andere Steuerelemente, die Teil Ihrer aktivierten Standards sind (einschließlich neu veröffentlichter Steuerelemente), sind deaktiviert. Wenn Sie DisabledSecurityControlIdentifiers diese Option wählen, sind die angegebenen Steuerelemente deaktiviert. Andere Steuerelemente, die Teil Ihrer aktivierten Standards sind (einschließlich neu veröffentlichter Steuerelemente), sind aktiviert.
6. Geben Sie optional für das SecurityControlCustomParameters Feld aktivierte Steuerelemente an, für die Sie Parameter anpassen möchten. Geben Sie CUSTOM das ValueType Feld und den benutzerdefinierten Parameterwert für das Value Feld an. Der Wert muss dem richtigen Datentyp entsprechen und innerhalb der von Security Hub CSPM angegebenen gültigen Bereiche liegen. Nur ausgewählte Steuerelemente unterstützen benutzerdefinierte Parameterwerte. Weitere Informationen finden Sie unter [Grundlegendes zu den Steuerparametern in Security Hub CSPM](#).
7. Um Ihre Konfigurationsrichtlinie auf Konten anzuwenden oder OUs rufen Sie die [StartConfigurationPolicyAssociation](#) API über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion auf.

8. Geben Sie für das `ConfigurationPolicyIdentifier` Feld den Amazon-Ressourcennamen (ARN) oder die Universally Unique Identifier (UUID) der Richtlinie ein. Der ARN und die UUID werden von der `CreateConfigurationPolicy` API zurückgegeben. Bei einer selbstverwalteten Konfiguration entspricht das `ConfigurationPolicyIdentifier` Feld `SELF_MANAGED_SECURITY_HUB`.
9. Geben Sie für das `Target` Feld die Organisationseinheit, das Konto oder die Root-ID an, für die diese Konfigurationsrichtlinie gelten soll. Sie können in jeder API-Anfrage nur ein Ziel angeben. Untergeordnete Konten und Konten OUs des ausgewählten Ziels erben diese Konfigurationsrichtlinie automatisch, sofern sie nicht selbst verwaltet werden oder eine andere Konfigurationsrichtlinie verwenden.

Beispiel für eine API-Anfrage zur Erstellung einer Konfigurationsrichtlinie:

```
{
  "Name": "SampleConfigurationPolicy",
  "Description": "Configuration policy for production accounts",
  "ConfigurationPolicy": {
    "SecurityHub": {
      "ServiceEnabled": true,
      "EnabledStandardIdentifiers": [
        "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
        "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
      ],
      "SecurityControlsConfiguration": {
        "DisabledSecurityControlIdentifiers": [
          "CloudTrail.2"
        ],
        "SecurityControlCustomParameters": [
          {
            "SecurityControlId": "ACM.1",
            "Parameters": {
              "daysToExpiration": {
                "ValueType": "CUSTOM",
                "Value": {
                  "Integer": 15
                }
              }
            }
          }
        ]
      }
    }
  }
}
```

```

    }
  }
}
]

```

Beispiel für eine API-Anfrage zum Zuordnen einer Konfigurationsrichtlinie:

```

{
  "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Target": {"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}
}

```

AWS CLI

Um Konfigurationsrichtlinien zu erstellen und zuzuordnen

1. Führen Sie den [create-configuration-policy](#) Befehl über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion aus.
2. Geben Sie für name einen eindeutigen Namen für die Konfigurationsrichtlinie ein. Geben Sie optional für description eine Beschreibung der Konfigurationsrichtlinie an.
3. Geben Sie für das ServiceEnabled Feld an, ob Security Hub CSPM in dieser Konfigurationsrichtlinie aktiviert oder deaktiviert werden soll.
4. Geben Sie für das EnabledStandardIdentifiers Feld an, welche Security Hub CSPM-Standards Sie in dieser Konfigurationsrichtlinie aktivieren möchten.
5. Geben Sie für das SecurityControlsConfiguration Feld an, welche Steuerelemente Sie in dieser Konfigurationsrichtlinie aktivieren oder deaktivieren möchten. Wählen Sie EnabledSecurityControlIdentifiers aus, dass die angegebenen Steuerelemente aktiviert sind. Andere Steuerelemente, die Teil Ihrer aktivierten Standards sind (einschließlich neu veröffentlichter Steuerelemente), sind deaktiviert. Wenn Sie DisabledSecurityControlIdentifiers diese Option wählen, sind die angegebenen Steuerelemente deaktiviert. Andere Steuerelemente, die Ihren aktivierten Standards entsprechen (einschließlich neu veröffentlichter Steuerelemente), sind aktiviert.
6. Geben Sie optional für das SecurityControlCustomParameters Feld aktivierte Steuerelemente an, für die Sie Parameter anpassen möchten. Geben Sie CUSTOM das

ValueType Feld und den benutzerdefinierten Parameterwert für das Value Feld an. Der Wert muss dem richtigen Datentyp entsprechen und innerhalb der von Security Hub CSPM angegebenen gültigen Bereiche liegen. Nur ausgewählte Steuerelemente unterstützen benutzerdefinierte Parameterwerte. Weitere Informationen finden Sie unter [Grundlegendes zu den Steuerparametern in Security Hub CSPM](#).

7. Um Ihre Konfigurationsrichtlinie auf Konten anzuwenden OUs, oder führen Sie den [start-configuration-policy-association](#) Befehl über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion aus.
8. Geben Sie für das configuration-policy-identifizier Feld den Amazon-Ressourcennamen (ARN) oder die ID der Konfigurationsrichtlinie ein. Dieser ARN und diese ID werden vom create-configuration-policy Befehl zurückgegeben.
9. Geben Sie für das target Feld die Organisationseinheit, das Konto oder die Root-ID an, für die diese Konfigurationsrichtlinie gelten soll. Sie können jedes Mal, wenn Sie den Befehl ausführen, nur ein Ziel angeben. Untergeordnete Objekte des ausgewählten Ziels erben diese Konfigurationsrichtlinie automatisch, sofern sie nicht selbst verwaltet werden oder eine andere Konfigurationsrichtlinie verwenden.

Beispielbefehl zum Erstellen einer Konfigurationsrichtlinie:

```
aws securityhub --region us-east-1 create-configuration-policy \
--name "SampleConfigurationPolicy" \
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
"EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0", "arn:aws:securityhub::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"], "SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
"SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
{"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}]}}}'
```

Beispielbefehl zum Zuordnen einer Konfigurationsrichtlinie:

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifizier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}'
```

Die `StartConfigurationPolicyAssociation` API gibt ein Feld namens `zurückAssociationStatus`. In diesem Feld erfahren Sie, ob eine Richtlinienverknüpfung noch aussteht oder ob sie erfolgreich oder nicht erfolgreich ist. Es kann bis zu 24 Stunden dauern, bis sich der Status von `PENDING` zu `SUCCESS` oder ändert `FAILURE`. Weitere Informationen zum Zuordnungsstatus finden Sie unter [Überprüfen Sie den Zuordnungsstatus einer Konfigurationsrichtlinie](#).

Überprüfen des Status und der Details der Konfigurationsrichtlinien

Der delegierte AWS Security Hub Cloud Security Posture Management (CSPM) -Administrator kann die Konfigurationsrichtlinien für eine Organisation und deren Details einsehen. Dazu gehört, mit welchen Konten und Organisationseinheiten (OUs) eine Richtlinie verknüpft ist.

Hintergrundinformationen zu den Vorteilen der zentralen Konfiguration und ihrer Funktionsweise finden Sie unter [Grundlegendes zur zentralen Konfiguration in Security Hub CSPM](#).

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um Ihre Konfigurationsrichtlinien einzusehen.

Security Hub CSPM console

So zeigen Sie die Konfigurationsrichtlinien an (Konsole)

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>

Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub CSPM-Administratorkontos in der Heimatregion an.

2. Wählen Sie im Navigationsbereich Einstellungen und Konfiguration aus.
3. Wählen Sie die Registerkarte Richtlinien, um einen Überblick über Ihre Konfigurationsrichtlinien zu erhalten.
4. Wählen Sie eine Konfigurationsrichtlinie aus und klicken Sie auf Details anzeigen, um weitere Informationen zu dieser Richtlinie anzuzeigen, einschließlich der Konten, mit denen OUs sie verknüpft ist.

Security Hub CSPM API

Um eine zusammenfassende Liste all Ihrer Konfigurationsrichtlinien anzuzeigen, verwenden Sie den [ListConfigurationPolicies](#) Betrieb der Security Hub CSPM-API. Wenn Sie den verwenden AWS

CLI, führen Sie den [list-configuration-policies](#) Befehl aus. Das delegierte Security Hub CSPM-Administratorkonto sollte den Vorgang in der Heimatregion aufrufen.

```
$ aws securityhub list-configuration-policies \
--max-items 5 \
--starting-token U2FsdGVkX19nUI2zoh+Pou9YyutLYJHWpn9xnG4hqS0hvw3o2JqjI23QDxdf
```

Verwenden Sie den Vorgang, um Details zu einer bestimmten Konfigurationsrichtlinie anzuzeigen. [GetConfigurationPolicy](#) Wenn Sie den verwenden AWS CLI, führen Sie den aus [get-configuration-policy](#). Das delegierte Administratorkonto sollte den Vorgang in der Heimatregion aufrufen. Geben Sie den Amazon-Ressourcennamen (ARN) oder die ID der Konfigurationsrichtlinie ein, deren Details Sie sehen möchten.

```
$ aws securityhub get-configuration-policy \
--identifizier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Verwenden Sie den [ListConfigurationPolicyAssociations](#) Vorgang, um eine zusammenfassende Liste all Ihrer Konfigurationsrichtlinien und ihrer Kontozuordnungen anzuzeigen. Wenn Sie den verwenden AWS CLI, führen Sie den [list-configuration-policy-associations](#) Befehl aus. Das delegierte Administratorkonto sollte den Vorgang in der Heimatregion aufrufen. Optional können Sie Paginierungsparameter angeben oder die Ergebnisse nach einer bestimmten Richtlinien-ID, einem Zuordnungstyp oder einem Zuordnungsstatus filtern.

```
$ aws securityhub list-configuration-policy-associations \
--filters '{"AssociationType": "APPLIED"}'
```

Verwenden Sie den [GetConfigurationPolicyAssociation](#) Vorgang, um Verknüpfungen für ein bestimmtes Konto anzuzeigen. Wenn Sie den verwenden AWS CLI, führen Sie den [get-configuration-policy-association](#) Befehl aus. Das delegierte Administratorkonto sollte den Vorgang in der Heimatregion aufrufen. Geben Sie für target die Kontonummer, OU-ID oder Root-ID an.

```
$ aws securityhub get-configuration-policy-association \
--target '{"AccountId": "123456789012"}'
```

Überprüfen Sie den Zuordnungsstatus einer Konfigurationsrichtlinie

Die folgenden API-Operationen für die zentrale Konfiguration geben ein Feld mit dem Namen `AssociationStatus` zurück:

- `BatchGetConfigurationPolicyAssociations`
- `GetConfigurationPolicyAssociation`
- `ListConfigurationPolicyAssociations`
- `StartConfigurationPolicyAssociation`

Dieses Feld wird sowohl zurückgegeben, wenn es sich bei der zugrunde liegenden Konfiguration um eine Konfigurationsrichtlinie handelt, als auch wenn es sich um ein selbstverwaltetes Verhalten handelt.

Der Wert von `AssociationStatus` gibt an, ob eine Richtlinienzuweisung für ein bestimmtes Konto noch aussteht oder ob sie erfolgreich oder nicht erfolgreich ist. Es kann bis zu 24 Stunden dauern, bis sich der Status von `PENDING` zu `SUCCESS` oder `FAILED` ändert. Ein Status von `SUCCESS` bedeutet, dass alle in der Konfigurationsrichtlinie angegebenen Einstellungen dem Konto zugeordnet sind. Ein Status von `FAILED` bedeutet, dass eine oder mehrere in der Konfigurationsrichtlinie angegebene Einstellungen dem Konto nicht zugeordnet werden konnten. Trotz eines `FAILED` Status konnte das Konto gemäß der Richtlinie teilweise konfiguriert werden. Sie könnten beispielsweise versuchen, ein Konto mit einer Konfigurationsrichtlinie zu verknüpfen, die Security Hub CSPM aktiviert, AWS Foundational Security Best Practices aktiviert und .1 deaktiviert. CloudTrail Die ersten beiden Einstellungen könnten erfolgreich sein, aber die Einstellung CloudTrail .1 könnte fehlschlagen. In diesem Beispiel lautet der Zuordnungsstatus, `FAILED` obwohl einige Einstellungen korrekt konfiguriert wurden.

Der Zuordnungsstatus einer übergeordneten Organisationseinheit oder der Stammorganisation hängt vom Status ihrer untergeordneten Organisationseinheiten ab. Wenn der Assoziationsstatus aller Kinder lautet `SUCCESS`, ist der Assoziationsstatus des Elternteils `SUCCESS`. Wenn der Assoziationsstatus eines oder mehrerer Kinder lautet `FAILED`, ist der Assoziationsstatus des Elternteils `FAILED`.

Der Wert von `AssociationStatus` hängt vom Assoziationsstatus der Police in allen relevanten Regionen ab. Wenn die Assoziation in der Heimatregion und allen verbundenen Regionen erfolgreich ist, ist `AssociationStatus` `SUCCESS` der Wert von. Wenn die Zuordnung in einer oder mehreren dieser Regionen fehlschlägt, ist `AssociationStatus` `FAILED` der Wert von.

Das folgende Verhalten wirkt sich auch auf den Wert von `ausAssociationStatus`:

- Handelt es sich bei dem Ziel um eine übergeordnete Organisationseinheit oder um die Stammorganisation, hat sie nur dann den `AssociationStatus` Wert „Ein“ `SUCCESS` oder „`FAILED`“, wenn alle untergeordneten Organisationseinheiten den `FAILED` Status „`SUCCESS`“ haben. Wenn sich der Zuordnungsstatus eines untergeordneten Kontos oder einer Organisationseinheit ändert (z. B. wenn eine verknüpfte Region hinzugefügt oder entfernt wird), nachdem Sie das übergeordnete Konto mit einer Konfiguration verknüpft haben, wird durch die Änderung der Zuordnungsstatus des übergeordneten Kontos nicht aktualisiert, es sei denn, Sie rufen die `StartConfigurationPolicyAssociation` API erneut auf.
- Handelt es sich bei dem Ziel um ein Konto, hat es den `AssociationStatus` Wert „Von“ `SUCCESS` oder `FAILED` nur, wenn die Zuordnung ein Ergebnis von `SUCCESS` oder `FAILED` in der Heimatregion und allen verknüpften Regionen hat. Wenn sich der Zuordnungsstatus eines Zielkontos ändert (z. B. wenn eine verknüpfte Region hinzugefügt oder entfernt wird), nachdem Sie es zum ersten Mal mit einer Konfiguration verknüpft haben, wird sein Zuordnungsstatus aktualisiert. Durch die Änderung wird der Zuordnungsstatus des übergeordneten Elements jedoch nicht aktualisiert, es sei denn, Sie rufen die `StartConfigurationPolicyAssociation` API erneut auf.

Wenn Sie eine neue verknüpfte Region hinzufügen, repliziert Security Hub CSPM Ihre vorhandenen Verknüpfungen, die sich in einem `PENDINGSUCCESS`, oder `FAILED` Bundesstaat der neuen Region befinden.

Selbst wenn der Zuordnungsstatus lautet `SUCCESS`, kann der Aktivierungsstatus eines Standards, der Teil der Richtlinie ist, in einen unvollständigen Status übergehen. In diesem Fall kann Security Hub CSPM keine Ergebnisse für die Kontrollen des Standards generieren. Weitere Informationen finden Sie unter [Den Status eines Standards überprüfen](#).

Behebung eines Zuordnungsfehlers

In AWS Security Hub Cloud Security Posture Management (CSPM) kann eine Zuordnung von Konfigurationsrichtlinien aus den folgenden häufigen Gründen fehlschlagen.

- Das Organisationsverwaltungskonto ist kein Mitglied — Wenn Sie dem Organisationsverwaltungskonto eine Konfigurationsrichtlinie zuordnen möchten, muss für dieses Konto bereits AWS Security Hub Cloud Security Posture Management (CSPM) aktiviert sein. Dadurch wird das Verwaltungskonto zu einem Mitgliedskonto in der Organisation.

- AWS Config ist nicht aktiviert oder nicht richtig konfiguriert — Um Standards in einer Konfigurationsrichtlinie zu aktivieren, AWS Config muss sie aktiviert und konfiguriert sein, um relevante Ressourcen aufzuzeichnen.
- Die Verknüpfung muss über ein delegiertes Administratorkonto erfolgen — Sie können eine Richtlinie nur Zielkonten zuordnen und OUs wenn Sie mit dem delegierten Security Hub CSPM-Administratorkonto angemeldet sind.
- Verbindung muss von der Heimatregion aus erfolgen — Sie können eine Richtlinie nur Zielkonten zuordnen und nur, OUs wenn Sie in Ihrer Heimatregion angemeldet sind.
- Opt-in-Region nicht aktiviert — Die Richtlinienverknüpfung schlägt für ein Mitgliedskonto oder eine Organisationseinheit in einer verknüpften Region fehl, wenn es sich um eine Opt-in-Region handelt, die der delegierte Administrator nicht aktiviert hat. Sie können es erneut versuchen, nachdem Sie die Region über das delegierte Administratorkonto aktiviert haben.
- Mitgliedskonto gesperrt — Die Richtlinienverknüpfung schlägt fehl, wenn Sie versuchen, eine Richtlinie mit einem gesperrten Mitgliedskonto zu verknüpfen.

Aktualisierung der Konfigurationsrichtlinien

Nach der Erstellung einer Konfigurationsrichtlinie kann das delegierte AWS Security Hub Cloud Security Posture Management (CSPM) -Administratorkonto die Richtliniendetails und Richtlinienzuordnungen aktualisieren. Wenn die Richtliniendetails aktualisiert werden, verwenden Konten, die der Konfigurationsrichtlinie zugeordnet sind, automatisch die aktualisierte Richtlinie.

Hintergrundinformationen zu den Vorteilen der zentralen Konfiguration und ihrer Funktionsweise finden Sie unter [Grundlegendes zur zentralen Konfiguration in Security Hub CSPM](#).

Der delegierte Administrator kann die folgenden Richtlinieneinstellungen aktualisieren:

- Aktivieren oder deaktivieren Sie Security Hub CSPM.
- Aktivieren Sie einen oder mehrere [Sicherheitsstandards](#).
- Geben Sie an, welche [Sicherheitskontrollen](#) für alle aktivierten Standards aktiviert sind. Sie können dies tun, indem Sie eine Liste bestimmter Steuerelemente bereitstellen, die aktiviert werden sollten, und Security Hub CSPM deaktiviert alle anderen Steuerelemente, einschließlich neuer Steuerelemente, wenn sie veröffentlicht werden. Alternativ können Sie eine Liste mit bestimmten Steuerelementen bereitstellen, die deaktiviert werden sollten, und Security Hub CSPM aktiviert alle anderen Kontrollen, einschließlich neuer Steuerelemente, wenn sie veröffentlicht werden.

- [Passen Sie optional die Parameter](#) für ausgewählte aktivierte Steuerelemente für alle aktivierten Standards an.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten zum Aktualisieren einer Konfigurationsrichtlinie.

 Note

Wenn Sie die zentrale Konfiguration verwenden, deaktiviert Security Hub CSPM automatisch Kontrollen, die globale Ressourcen in allen Regionen außer der Heimatregion betreffen. Andere Steuerelemente, die Sie über eine Konfigurationsrichtlinie aktivieren, sind in allen Regionen aktiviert, in denen sie verfügbar sind. Um die Ergebnisse für diese Steuerelemente auf nur eine Region zu beschränken, können Sie Ihre AWS Config Rekordereinstellungen aktualisieren und die globale Ressourcenaufzeichnung in allen Regionen außer der Heimatregion deaktivieren.

Wenn ein aktiviertes Steuerelement, das globale Ressourcen umfasst, in der Heimatregion nicht unterstützt wird, versucht Security Hub CSPM, das Steuerelement in einer verknüpften Region zu aktivieren, in der das Steuerelement unterstützt wird. Bei zentraler Konfiguration fehlt Ihnen die Abdeckung für ein Steuerelement, das in der Heimatregion oder einer der verknüpften Regionen nicht verfügbar ist.

Eine Liste der Steuerelemente, die globale Ressourcen betreffen, finden Sie unter [Kontrollen, die globale Ressourcen verwenden](#).

Console

So aktualisieren Sie die Konfigurationsrichtlinien

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>

Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub CSPM-Administratorkontos in der Heimatregion an.

2. Wählen Sie im Navigationsbereich Einstellungen und Konfiguration aus.
3. Wählen Sie die Registerkarte Policies.
4. Wählen Sie die Konfigurationsrichtlinie aus, die Sie bearbeiten möchten, und wählen Sie Bearbeiten aus. Falls gewünscht, bearbeiten Sie die Richtlinieneinstellungen. Lassen Sie

diesen Abschnitt unverändert, wenn Sie die Richtlinienereinstellungen unverändert lassen möchten.

5. Wählen Sie Weiter. Falls gewünscht, bearbeiten Sie die Richtlinienverknüpfungen. Lassen Sie diesen Abschnitt unverändert, wenn Sie die Richtlinienverknüpfungen unverändert lassen möchten. Sie können die Richtlinie bei der Aktualisierung maximal 15 Zielen (Konten oder Root) zuordnen oder deren Zuordnung aufheben. OUs
6. Wählen Sie Weiter aus.
7. Überprüfen Sie Ihre Änderungen und wählen Sie Speichern und anwenden. In Ihrer Heimatregion und den verknüpften Regionen setzt diese Aktion die vorhandenen Konfigurationseinstellungen der Konten außer Kraft, die dieser Konfigurationsrichtlinie zugeordnet sind. Konten können über eine Anwendung oder durch Vererbung von einem übergeordneten Knoten mit einer Konfigurationsrichtlinie verknüpft werden.

API

Um die Konfigurationsrichtlinien zu aktualisieren

1. Um die Einstellungen in einer Konfigurationsrichtlinie zu aktualisieren, rufen Sie die [UpdateConfigurationPolicy](#) API über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion auf.
2. Geben Sie den Amazon-Ressourcennamen (ARN) oder die ID der Konfigurationsrichtlinie an, die Sie aktualisieren möchten.
3. Geben Sie aktualisierte Werte für die Felder unter `ConfigurationPolicy`. Optional können Sie auch einen Grund für die Aktualisierung angeben.
4. Um neue Verknüpfungen für diese Konfigurationsrichtlinie hinzuzufügen, rufen Sie die [StartConfigurationPolicyAssociation](#) API über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion auf. Um eine oder mehrere aktuelle Verknüpfungen zu entfernen, rufen Sie die [StartConfigurationPolicyDisassociation](#) API über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion auf.
5. Geben Sie für das `ConfigurationPolicyIdentifier` Feld den ARN oder die ID der Konfigurationsrichtlinie ein, deren Verknüpfungen Sie aktualisieren möchten.
6. Geben Sie für das `Target` Feld die Konten oder die Root-ID ein, die Sie zuordnen oder trennen möchten. OUs Diese Aktion setzt vorherige Richtlinienzuordnungen für die angegebenen OUs Konten außer Kraft.

Note

Wenn Sie die `UpdateConfigurationPolicy` API aufrufen, führt Security Hub CSPM eine vollständige Listenersetzung für die Felder `EnabledStandardIdentifiers`, `EnabledSecurityControlIdentifiers`, `DisabledSecurityControlIdentifiers`, und durch `SecurityControlCustomParameters`. Geben Sie bei jedem Aufruf dieser API die vollständige Liste der Standards an, die Sie aktivieren möchten, sowie die vollständige Liste der Steuerelemente, die Sie aktivieren oder deaktivieren und deren Parameter anpassen möchten.

Beispiel für eine API-Anfrage zur Aktualisierung einer Konfigurationsrichtlinie:

```
{
  "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Description": "Updated configuration policy",
  "UpdatedReason": "Disabling CloudWatch.1",
  "ConfigurationPolicy": {
    "SecurityHub": {
      "ServiceEnabled": true,
      "EnabledStandardIdentifiers": [
        "arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0",
        "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0"
      ],
      "SecurityControlsConfiguration": {
        "DisabledSecurityControlIdentifiers": [
          "CloudTrail.2",
          "CloudWatch.1"
        ],
        "SecurityControlCustomParameters": [
          {
            "SecurityControlId": "ACM.1",
            "Parameters": {
              "daysToExpiration": {
                "ValueType": "CUSTOM",
                "Value": {
                  "Integer": 15
                }
              }
            }
          }
        ]
      }
    }
  }
}
```

AWS CLI

Um die Konfigurationsrichtlinien zu aktualisieren

1. Um die Einstellungen in einer Konfigurationsrichtlinie zu aktualisieren, führen Sie den [update-configuration-policy](#)Befehl über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion aus.
2. Geben Sie den Amazon-Ressourcennamen (ARN) oder die ID der Konfigurationsrichtlinie an, die Sie aktualisieren möchten.
3. Geben Sie aktualisierte Werte für die Felder unter `inconfiguration-policy`. Optional können Sie auch einen Grund für die Aktualisierung angeben.
4. Um neue Verknüpfungen für diese Konfigurationsrichtlinie hinzuzufügen, führen Sie den [start-configuration-policy-association](#)Befehl über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion aus. Um eine oder mehrere aktuelle Verknüpfungen zu entfernen, führen Sie den [start-configuration-policy-disassociation](#)Befehl über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion aus.
5. Geben Sie für das `configuration-policy-identifier` Feld den ARN oder die ID der Konfigurationsrichtlinie ein, deren Verknüpfungen Sie aktualisieren möchten.
6. Geben Sie für das `target` Feld die Konten oder die Root-ID ein, die Sie zuordnen oder trennen möchten. OUs Diese Aktion setzt vorherige Richtlinienzuordnungen für die angegebenen OUs Konten außer Kraft.

 Note

Wenn Sie den `update-configuration-policy` Befehl ausführen, führt Security Hub CSPM eine vollständige Listenerersetzung für die Felder `EnabledStandardIdentifiers`, `EnabledSecurityControlIdentifiers` und `DisabledSecurityControlIdentifiers`.

und `SecurityControlCustomParameters` durch. Geben Sie bei jeder Ausführung dieses Befehls die vollständige Liste der Standards an, die Sie aktivieren möchten, sowie die vollständige Liste der Steuerelemente, die Sie aktivieren oder deaktivieren möchten, und für die Sie die Parameter anpassen möchten.

Beispielbefehl zum Aktualisieren einer Konfigurationsrichtlinie:

```
aws securityhub update-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--description "Updated configuration policy" \
--updated-reason "Disabling CloudWatch.1" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
  "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0","arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0"], "SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2","CloudWatch.1"],
  "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
{"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}}]}}}'
```

Die `StartConfigurationPolicyAssociation` API gibt ein Feld namens `AssociationStatus`. In diesem Feld erfahren Sie, ob eine Richtlinienverknüpfung noch aussteht oder ob sie erfolgreich oder nicht erfolgreich ist. Es kann bis zu 24 Stunden dauern, bis sich der Status von `PENDING` zu `SUCCESS` oder ändert `FAILURE`. Weitere Informationen zum Zuordnungsstatus finden Sie unter [Überprüfen Sie den Zuordnungsstatus einer Konfigurationsrichtlinie](#).

Löschen von Konfigurationsrichtlinien

Nach der Erstellung einer Konfigurationsrichtlinie kann der delegierte AWS Security Hub Cloud Security Posture Management (CSPM) -Administrator diese löschen. Alternativ kann der delegierte Administrator die Richtlinie beibehalten, sie jedoch von bestimmten Konten oder Organisationseinheiten (OUs) oder vom Stammverzeichnis trennen. Anweisungen zum Aufheben der Zuordnung zu einer Richtlinie finden Sie unter [Aufheben der Zuordnung einer Konfiguration zu ihren Zielen](#).

Hintergrundinformationen zu den Vorteilen der zentralen Konfiguration und ihrer Funktionsweise finden Sie unter. [Grundlegendes zur zentralen Konfiguration in Security Hub CSPM](#)

In diesem Abschnitt wird erklärt, wie Konfigurationsrichtlinien gelöscht werden.

Wenn Sie eine Konfigurationsrichtlinie löschen, ist sie für Ihre Organisation nicht mehr vorhanden. Zielkonten und der Organisationsstamm können die Konfigurationsrichtlinie nicht mehr verwenden. OUs Ziele, die mit einer gelöschten Konfigurationsrichtlinie verknüpft waren, erben die Konfigurationsrichtlinie des nächstgelegenen übergeordneten Objekts oder werden selbst verwaltet, wenn das nächstgelegene übergeordnete Objekt selbst verwaltet wird. Wenn Sie möchten, dass ein Ziel eine andere Konfiguration verwendet, können Sie das Ziel einer neuen Konfigurationsrichtlinie zuordnen. Weitere Informationen finden Sie unter [Konfigurationsrichtlinien erstellen und zuordnen](#).

Wir empfehlen, mindestens eine Konfigurationsrichtlinie zu erstellen und mit Ihrer Organisation zu verknüpfen, um einen angemessenen Sicherheitsschutz zu gewährleisten.

Bevor Sie eine Konfigurationsrichtlinie löschen können, müssen Sie die Zuordnung der Richtlinie zu allen Konten oder dem Stammkonto OUs aufheben, für das sie derzeit gilt.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten zum Löschen einer Konfigurationsrichtlinie.

Console

Um eine Konfigurationsrichtlinie zu löschen

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>

Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub CSPM-Administratorkontos in der Heimatregion an.

2. Wählen Sie im Navigationsbereich Einstellungen und Konfiguration aus.
3. Wählen Sie die Registerkarte Policies. Wählen Sie die Konfigurationsrichtlinie aus, die Sie löschen möchten, und wählen Sie Löschen aus. Wenn die Konfigurationsrichtlinie noch mit Konten oder verknüpft ist OUs, werden Sie aufgefordert, die Richtlinie zunächst von diesen Zielen zu trennen, bevor Sie sie löschen können.
4. Überprüfen Sie die Bestätigungsnachricht. Geben Sie ein **confirm** und wählen Sie Löschen.

API

Um eine Konfigurationsrichtlinie zu löschen

Rufen Sie die [DeleteConfigurationPolicy](#) API über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion auf.

Geben Sie den Amazon-Ressourcennamen (ARN) oder die ID der Konfigurationsrichtlinie an, die Sie löschen möchten. Wenn Sie eine `ConflictException` Fehlermeldung erhalten, gilt die Konfigurationsrichtlinie weiterhin für Konten oder OUs in Ihrer Organisation. Um den Fehler zu beheben, trennen Sie die Konfigurationsrichtlinie von diesen Konten oder OUs bevor Sie versuchen, sie zu löschen.

Beispiel für eine API-Anfrage zum Löschen einer Konfigurationsrichtlinie:

```
{
  "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

AWS CLI

Um eine Konfigurationsrichtlinie zu löschen

Führen Sie den [delete-configuration-policy](#) Befehl über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion aus.

Geben Sie den Amazon-Ressourcennamen (ARN) oder die ID der Konfigurationsrichtlinie an, die Sie löschen möchten. Wenn Sie eine `ConflictException` Fehlermeldung erhalten, gilt die Konfigurationsrichtlinie weiterhin für Konten oder OUs in Ihrer Organisation. Um den Fehler zu beheben, trennen Sie die Konfigurationsrichtlinie von diesen Konten oder OUs bevor Sie versuchen, sie zu löschen.

```
aws securityhub --region us-east-1 delete-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Aufheben der Zuordnung einer Konfiguration zu ihren Zielen

Über das delegierte AWS Security Hub Cloud Security Posture Management (CSPM) - Administratorkonto können Sie die Zuordnung einer Konfigurationsrichtlinie oder einer selbstverwalteten Konfiguration zu einem Konto, einer Organisationseinheit oder einem Root-Konto aufheben. Durch die Trennung der Zuordnung wird die Richtlinie für die future Verwendung beibehalten, bestehende Verknüpfungen zu bestimmten Konten oder dem Stammkonto werden jedoch entfernt. Sie können nur eine direkt angewendete Konfiguration trennen, keine vererbte Konfiguration. OUs Um eine geerbte Konfiguration zu ändern, können Sie eine Konfigurationsrichtlinie oder ein selbstverwaltetes Verhalten auf das betroffene Konto oder die betroffene Organisationseinheit anwenden. Sie können auch eine neue Konfigurationsrichtlinie, die Ihre gewünschten Änderungen enthält, auf das nächstgelegene übergeordnete Objekt anwenden.

Durch die Trennung der Zuordnung wird eine Konfigurationsrichtlinie nicht gelöscht. Die Richtlinie wird in Ihrem Konto gespeichert, sodass Sie sie mit anderen Zielen in Ihrer Organisation verknüpfen können. Anweisungen zum Löschen einer Konfigurationsrichtlinie finden Sie unter [Löschen von Konfigurationsrichtlinien](#). Wenn die Trennung abgeschlossen ist, erbt ein betroffenes Ziel die Konfigurationsrichtlinie oder das selbstverwaltete Verhalten des nächstgelegenen übergeordneten Ziels. Wenn es keine vererbte Konfiguration gibt, behält ein Ziel die Einstellungen bei, die es vor der Trennung hatte, wird aber selbst verwaltet.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um ein Konto, eine Organisationseinheit oder einen Root-Benutzer von der aktuellen Konfiguration zu trennen.

Console

Um ein Konto oder eine Organisationseinheit von der aktuellen Konfiguration zu trennen

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>

Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub CSPM-Administratorkontos in der Heimatregion an.

2. Wählen Sie im Navigationsbereich Einstellungen und Konfiguration aus.
3. Wählen Sie auf der Registerkarte Organizations das Konto, die Organisationseinheit oder das Stammverzeichnis aus, das Sie von der aktuellen Konfiguration trennen möchten. Wählen Sie Bearbeiten aus.

4. Wählen Sie auf der Seite Konfiguration definieren für Verwaltung die Option Anwendete Richtlinie aus, wenn Sie möchten, dass der delegierte Administrator Richtlinien direkt auf das Ziel anwenden kann. Wählen Sie Vererbt, wenn Sie möchten, dass das Ziel die Konfiguration seines nächsten übergeordneten Objekts erbt. In beiden Fällen kontrolliert der delegierte Administrator die Einstellungen für das Ziel. Wählen Sie Selbstverwaltet, wenn Sie möchten, dass das Konto oder die Organisationseinheit ihre eigenen Einstellungen steuert.
5. Nachdem Sie Ihre Änderungen überprüft haben, wählen Sie Weiter und Anwenden. Diese Aktion überschreibt bestehende Konfigurationen aller Konten oder Konten OUs , die sich im Gültigkeitsbereich befinden, falls diese Konfigurationen mit Ihrer aktuellen Auswahl in Konflikt stehen.

API

Um die Zuordnung eines Kontos oder einer Organisationseinheit zu ihrer aktuellen Konfiguration aufzuheben

1. Rufen Sie die [StartConfigurationPolicyDisassociation](#) API über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion auf.
2. Geben Sie für `ConfigurationPolicyIdentifier` den Amazon-Ressourcennamen (ARN) oder die ID der Konfigurationsrichtlinie an, deren Zuordnung Sie aufheben möchten. Geben Sie dieses Feld an, `SELF_MANAGED_SECURITY_HUB` um die Zuordnung zu selbstverwaltetem Verhalten aufzuheben.
3. Geben Sie für `Target` die Konten oder das Stammkonto an OUs, das Sie von dieser Konfigurationsrichtlinie trennen möchten.

Beispiel für eine API-Anfrage zum Trennen der Zuordnung zu einer Konfigurationsrichtlinie:

```
{
  "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Target": {"RootId": "r-f6g7h8i9j0example"}
}
```

AWS CLI

Um ein Konto oder eine Organisationseinheit von der aktuellen Konfiguration zu trennen

1. Führen Sie den [start-configuration-policy-disassociation](#) Befehl über das delegierte Security Hub-CSPM-Administratorkonto in der Heimatregion aus.
2. Geben Sie für `configuration-policy-identifizier` den Amazon-Ressourcennamen (ARN) oder die ID der Konfigurationsrichtlinie an, deren Zuordnung Sie aufheben möchten. Geben Sie dieses Feld an, `SELF_MANAGED_SECURITY_HUB` um die Zuordnung zu selbstverwaltetem Verhalten aufzuheben.
3. Geben Sie für `target` die Konten oder das Stammkonto an OUs, das Sie von dieser Konfigurationsrichtlinie trennen möchten.

Beispielbefehl zum Trennen der Zuordnung einer Konfigurationsrichtlinie:

```
aws securityhub --region us-east-1 start-configuration-policy-disassociation \
--configuration-policy-identifizier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"RootId": "r-f6g7h8i9j0example"}'
```

Konfiguration eines Standards oder einer Steuerung im Kontext

Wenn Sie die [zentrale Konfiguration](#) in AWS Security Hub Cloud Security Posture Management (CSPM) verwenden, kann der delegierte Security Hub CSPM-Administrator Konfigurationsrichtlinien erstellen, die festlegen, wie Security Hub CSPM, Sicherheitsstandards und Sicherheitskontrollen für eine Organisation konfiguriert werden. Der delegierte Administrator kann Richtlinien bestimmten Konten und Organisationseinheiten (OU) zuordnen. Die Richtlinien gelten in Ihrer Heimatregion und allen verknüpften Regionen. Der delegierte Administrator kann die Konfigurationsrichtlinien bei Bedarf aktualisieren.

Auf der Security Hub CSPM-Konsole kann der delegierte Administrator die Konfigurationsrichtlinien auf zwei Arten aktualisieren: von der Konfigurationsseite aus oder im Kontext mit bestehenden Workflows. Letzteres kann von Vorteil sein, da Sie anhand der Sicherheitsergebnisse herausfinden können, welche Standards und Kontrollen für Ihre Umgebung am relevantesten sind, und diese gleichzeitig konfigurieren können.

Die kontextabhängige Konfiguration ist nur auf der Security Hub CSPM-Konsole verfügbar. Programmgesteuert muss der delegierte Administrator den [UpdateConfigurationPolicy](#) Betrieb der Security Hub CSPM-API aufrufen, um die Konfiguration bestimmter Standards oder Kontrollen in der Organisation zu ändern.

Gehen Sie wie folgt vor, um einen Security Hub CSPM-Standard oder eine kontextbezogene Steuerung zu konfigurieren.

So konfigurieren Sie einen Standard oder ein kontextbezogenes Steuerelement (Konsole)

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>

Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub CSPM-Administratorkontos in der Heimatregion an.

2. Wählen Sie im Navigationsbereich eine der folgenden Optionen:
 - Um einen Standard zu konfigurieren, wählen Sie Sicherheitsstandards und dann einen bestimmten Standard aus.
 - Um ein Steuerelement zu konfigurieren, wählen Sie Controls und wählen Sie ein bestimmtes Steuerelement aus.
3. Die Konsole listet Ihre vorhandenen Security Hub CSPM-Konfigurationsrichtlinien und den Status des ausgewählten Standards oder Steuerelements in jeder Richtlinie auf. Wählen Sie in jeder vorhandenen Konfigurationsrichtlinie die Optionen aus, um den Standard oder die Steuerung zu aktivieren oder zu deaktivieren. Bei Steuerungen können Sie auch wählen, ob Sie die [Steuerparameter](#) anpassen möchten. Sie können während der kontextbezogenen Konfiguration keine neue Richtlinie erstellen. Um eine neue Richtlinie zu erstellen, müssen Sie zur Konfigurationsseite gehen, die Registerkarte Richtlinien und dann Richtlinie erstellen auswählen.
4. Nachdem Sie Ihre Änderungen vorgenommen haben, wählen Sie Weiter.
5. Überprüfen Sie Ihre Änderungen und wählen Sie Anwenden. Die Updates wirken sich auf alle Konten aus OUs, die mit einer geänderten Konfigurationsrichtlinie verknüpft sind. Die Updates werden auch in der Heimatregion und allen verknüpften Regionen wirksam.

Deaktivierung der zentralen Konfiguration in Security Hub CSPM

Wenn Sie die zentrale Konfiguration in AWS Security Hub Cloud Security Posture Management (CSPM) deaktivieren, verliert der delegierte Administrator die Möglichkeit, Security Hub CSPM, Sicherheitsstandards und Sicherheitskontrollen für mehrere AWS-Konten Organisationseinheiten () zu konfigurieren () und. OUs AWS-Regionen Stattdessen müssen Sie die meisten Einstellungen für jedes Konto in jeder Region separat konfigurieren.

Important

Bevor Sie die zentrale Konfiguration deaktivieren können, müssen Sie zuerst [Ihre Konten](#) [und](#) ihre aktuelle Konfiguration OUs trennen, unabhängig davon, ob es sich dabei um eine Konfigurationsrichtlinie oder ein selbstverwaltetes Verhalten handelt.

Bevor Sie die zentrale Konfiguration deaktivieren können, müssen Sie auch [vorhandene Konfigurationsrichtlinien löschen](#).

Wenn Sie die zentrale Konfiguration deaktivieren, treten die folgenden Änderungen auf:

- Der delegierte Administrator kann keine Konfigurationsrichtlinien mehr für die Organisation erstellen.
- Konten, auf die eine Konfigurationsrichtlinie angewendet oder vererbt wurde, behalten ihre aktuellen Einstellungen bei, werden jedoch automatisch verwaltet.
- Ihr Unternehmen wechselt zur lokalen Konfiguration. Bei der lokalen Konfiguration müssen die meisten Security Hub CSPM-Einstellungen für jedes Organisationskonto und jede Region separat konfiguriert werden. Der delegierte Administrator kann festlegen, dass Security Hub CSPM, [Standardsicherheitsstandards und alle Kontrollen, die Teil der Standardstandards](#) sind, in neuen Organisationskonten automatisch aktiviert werden. Die Standardstandards sind AWS Foundational Security Best Practices (FSBP) und Center for Internet Security (CIS) Foundations Benchmark v1.2.0. AWS Diese Einstellungen sind nur in der aktuellen Region wirksam und wirken sich nur auf neue Unternehmenskonten aus. Der delegierte Administrator kann nicht ändern, welche Standards die Standardstandards sind. Die lokale Konfiguration unterstützt nicht die Verwendung von Konfigurationsrichtlinien oder Konfigurationen auf OU-Ebene.

Die Identität des delegierten Administratorkontos bleibt unverändert, wenn Sie die zentrale Konfiguration nicht mehr verwenden. Ihre Heimatregion und die verknüpften Regionen bleiben

ebenfalls unverändert (Ihre Heimatregion wird jetzt als Aggregationsregion bezeichnet und kann für die Suche nach Aggregationen verwendet werden).

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um die zentrale Konfiguration nicht mehr zu verwenden und zur lokalen Konfiguration zu wechseln.

Security Hub CSPM console

Um die zentrale Konfiguration (Konsole) zu deaktivieren

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter: <https://console.aws.amazon.com/securityhub/>

Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub CSPM-Administratorkontos in der Heimatregion an.

2. Wählen Sie im Navigationsbereich Einstellungen und Konfiguration aus.
3. Wählen Sie im Abschnitt Übersicht die Option Bearbeiten aus.
4. Wählen Sie im Feld Organisationskonfiguration bearbeiten die Option Lokale Konfiguration aus. Falls Sie dies noch nicht getan haben, werden Sie aufgefordert, Ihre aktuellen Konfigurationsrichtlinien zu trennen und zu löschen, bevor Sie die zentrale Konfiguration beenden können. Konten oder Konten OUs, die als selbstverwaltet gekennzeichnet sind, müssen von ihrer selbstverwalteten Konfiguration getrennt werden. Sie können dies in der Konsole tun, indem Sie den [Verwaltungstyp jedes selbstverwalteten Kontos oder jeder Organisationseinheit auf Zentral verwaltet und von meiner Organisation übernehmen ändern](#).
5. Wählen Sie optional die Standardeinstellungen für die lokale Konfiguration für neue Organisationskonten aus.
6. Wählen Sie Bestätigen aus.

Security Hub CSPM API

Um die zentrale Konfiguration (API) zu deaktivieren

1. Rufen Sie die [UpdateOrganizationConfiguration](#)API auf.
2. Setzen Sie das ConfigurationType Feld im OrganizationConfiguration Objekt aufLOCAL. Die API gibt einen Fehler zurück, wenn Sie über bestehende Konfigurationsrichtlinien oder Richtlinienzuordnungen verfügen. Rufen Sie die API auf, um die Zuordnung einer Konfigurationsrichtlinie aufzuheben.

`StartConfigurationPolicyDisassociation` Rufen Sie die API auf, um eine Konfigurationsrichtlinie zu löschen. `DeleteConfigurationPolicy`

3. Wenn Sie Security Hub CSPM automatisch in neuen Organisationskonten aktivieren möchten, setzen Sie das `AutoEnable` Feld auf `true`. Standardmäßig ist der Wert dieses Felds `false`, und Security Hub CSPM wird nicht automatisch in neuen Organisationskonten aktiviert. Wenn Sie die Standardsicherheitsstandards für neue Organisationskonten automatisch aktivieren möchten, setzen Sie das `AutoEnableStandards` Feld optional auf `DEFAULT`. Dies ist der Standardwert. Wenn Sie die Standardsicherheitsstandards in neuen Organisationskonten nicht automatisch aktivieren möchten, setzen Sie das `AutoEnableStandards` Feld auf `NONE`.

Beispiel für eine API-Anfrage:

```
{
  "AutoEnable": true,
  "OrganizationConfiguration": {
    "ConfigurationType" : "LOCAL"
  }
}
```

AWS CLI

Um die zentrale Konfiguration zu deaktivieren (AWS CLI)

1. Führen Sie den Befehl [update-organization-configuration](#) aus.
2. Stellen Sie das `ConfigurationType` Feld im `organization-configuration` Objekt auf `LOCAL`. Der Befehl gibt einen Fehler zurück, wenn Sie bereits über Konfigurationsrichtlinien oder Richtlinienzuordnungen verfügen. Führen Sie den `start-configuration-policy-disassociation` Befehl aus, um die Zuordnung einer Konfigurationsrichtlinie aufzuheben. Führen Sie den `delete-configuration-policy` Befehl aus, um eine Konfigurationsrichtlinie zu löschen.
3. Wenn Sie Security Hub CSPM automatisch in neuen Organisationskonten aktivieren möchten, geben Sie den `auto-enable` Parameter an. Standardmäßig ist der Wert dieses Parameters `no-auto-enable`, und Security Hub CSPM wird nicht automatisch in neuen Organisationskonten aktiviert. Wenn Sie die Standardsicherheitsstandards für neue Organisationskonten automatisch aktivieren möchten, setzen Sie das `auto-`

`enable-standards` Feld optional auf `DEFAULT`. Dies ist der Standardwert. Wenn Sie die Standardsicherheitsstandards in neuen Organisationskonten nicht automatisch aktivieren möchten, setzen Sie das `auto-enable-standards` Feld auf `NONE`.

```
aws securityhub --region us-east-1 update-organization-configuration \  
--auto-enable \  
--organization-configuration '{"ConfigurationType": "LOCAL"}'
```

Verwaltung von Administrator- und Mitgliedskonten in Security Hub CSPM

Wenn Ihre AWS Umgebung über mehrere Konten verfügt, können Sie die Konten, die AWS Security Hub Cloud Security Posture Management (CSPM) verwenden, als Mitgliedskonten behandeln und sie einem einzigen Administratorkonto zuordnen. Der Administrator kann Ihren allgemeinen Sicherheitsstatus überwachen und [zulässige Aktionen](#) für Mitgliedskonten ergreifen. Der Administrator kann auch verschiedene Aufgaben zur Kontoverwaltung und -verwaltung in großem Umfang ausführen, z. B. die Überwachung der geschätzten Nutzungskosten und die Bewertung der Kontokontingente.

Sie können Mitgliedskonten auf zwei Arten einem Administrator zuordnen, indem Sie Security Hub CSPM in Security Hub CSPM integrieren AWS Organizations oder indem Sie Mitgliedschaftseinladungen manuell in Security Hub CSPM senden und annehmen.

Konten verwalten mit AWS Organizations

AWS Organizations ist ein globaler Kontoverwaltungsdienst, mit dem AWS Administratoren mehrere Konten konsolidieren und verwalten können. AWS-Konten Er bietet Funktionen zur Kontoverwaltung und konsolidierten Fakturierung, die auf die Erfüllung von Haushalts-, Sicherheits- und Compliance-Anforderungen zugeschnitten sind. Es wird ohne zusätzliche Kosten angeboten und lässt sich in mehrere integrieren AWS-Services, darunter AWS Security Hub Cloud Security Posture Management (CSPM), Amazon Macie und Amazon GuardDuty. Weitere Informationen finden Sie im [AWS Organizations -Benutzerhandbuch](#).

Wenn Sie Security Hub CSPM und integrieren AWS Organizations, bestimmt das Verwaltungskonto der Organizations einen delegierten Security Hub CSPM-Administrator. Security Hub CSPM wird automatisch in dem delegierten Administratorkonto aktiviert, AWS-Region in dem es zugewiesen wurde.

[Nach der Benennung eines delegierten Administrators empfehlen wir, Konten in Security Hub CSPM mit zentraler Konfiguration zu verwalten.](#) Dies ist die effizienteste Methode, Security Hub CSPM individuell anzupassen und eine angemessene Sicherheitsabdeckung für Ihr Unternehmen sicherzustellen.

Durch die zentrale Konfiguration kann der delegierte Administrator Security Hub CSPM für mehrere Unternehmenskonten und Regionen anpassen, anstatt es zu konfigurieren. Region-by-Region

Sie können eine Konfigurationsrichtlinie für Ihre gesamte Organisation oder unterschiedliche Konfigurationsrichtlinien für verschiedene Konten erstellen. OUs Die Richtlinien geben an, ob Security Hub CSPM in den zugehörigen Konten aktiviert oder deaktiviert ist und welche Sicherheitsstandards und Kontrollen aktiviert sind.

Der delegierte Administrator kann Konten als zentral verwaltete oder selbstverwaltete Konten festlegen. Zentral verwaltete Konten können nur vom delegierten Administrator konfiguriert werden. Selbstverwaltete Konten können ihre eigenen Einstellungen angeben.

Wenn Sie sich nicht für die zentrale Konfiguration entscheiden, hat der delegierte Administrator eine eingeschränkte Möglichkeit, Security Hub CSPM zu konfigurieren, was als lokale Konfiguration bezeichnet wird. Bei der lokalen Konfiguration kann der delegierte Administrator Security Hub CSPM und [Standardsicherheitsstandards](#) automatisch in neuen Unternehmenskonten in der aktuellen Region aktivieren. Bestehende Konten verwenden diese Einstellungen jedoch nicht, sodass es nach dem Beitritt eines Kontos zur Organisation zu Konfigurationsabweichungen kommen kann.

Abgesehen von diesen neuen Kontoeinstellungen ist die lokale Konfiguration konto- und regionsspezifisch. Jedes Organisationskonto muss den Security Hub CSPM-Dienst, die Standards und Kontrollen in jeder Region separat konfigurieren. Die lokale Konfiguration unterstützt auch nicht die Verwendung von Konfigurationsrichtlinien.

Manuelles Verwalten von Konten auf Einladung

Sie müssen Mitgliedskonten auf Einladung manuell in Security Hub CSPM verwalten, wenn Sie ein eigenständiges Konto haben oder wenn Sie nicht in Organizations integriert sind. Ein eigenständiges Konto kann nicht in Organizations integriert werden, daher muss es manuell verwaltet werden. Wir empfehlen, die zentrale Konfiguration zu integrieren AWS Organizations und diese zu verwenden, wenn Sie in future weitere Konten hinzufügen.

Wenn Sie die manuelle Kontoverwaltung verwenden, bestimmen Sie ein Konto als Security Hub CSPM-Administrator. Das Administratorkonto kann Daten in Mitgliedskonten einsehen und bestimmte Maßnahmen ergreifen, wenn die Ergebnisse des Mitgliedskontos berücksichtigt werden. Der Security Hub CSPM-Administrator lädt andere Konten als Mitgliedskonten ein, und die Beziehung zwischen Administrator und Mitglied wird hergestellt, wenn ein potenzielles Mitgliedskonto die Einladung annimmt.

Die manuelle Kontoverwaltung unterstützt die Verwendung von Konfigurationsrichtlinien nicht. Ohne Konfigurationsrichtlinien kann der Administrator Security Hub CSPM nicht zentral anpassen,

indem er variable Einstellungen für verschiedene Konten konfiguriert. Stattdessen muss jedes Organisationskonto Security Hub CSPM für sich selbst in jeder Region separat aktivieren und konfigurieren. Dies kann es schwieriger und zeitaufwändiger machen, eine angemessene Sicherheitsabdeckung für alle Konten und Regionen sicherzustellen, in denen Sie Security Hub CSPM verwenden. Dies kann auch zu Konfigurationsabweichungen führen, da Mitgliedskonten ihre eigenen Einstellungen ohne Eingaben des Administrators angeben können.

Informationen zur Verwaltung von Konten auf Einladung finden Sie unter [Konten auf Einladung in Security Hub CSPM verwalten](#).

Empfehlungen für die Verwaltung mehrerer Konten in Security Hub CSPM

Im folgenden Abschnitt werden einige Einschränkungen und Empfehlungen zusammengefasst, die Sie bei der Verwaltung von Mitgliedskonten in AWS Security Hub Cloud Security Posture Management (CSPM) beachten sollten.

Maximale Anzahl von Mitgliedern pro Konto

Wenn Sie die Integration mit verwenden AWS Organizations, unterstützt Security Hub CSPM jeweils bis zu 10.000 Mitgliedskonten pro delegiertem Administratorkonto. AWS-Region Wenn Sie Security Hub CSPM manuell aktivieren und verwalten, unterstützt Security Hub CSPM bis zu 1.000 Mitgliedskonteneinladungen pro Administratorkonto in jeder Region.

Beziehungen zwischen Administrator und Mitglied erstellen

Note

Wenn Sie die Security Hub CSPM-Integration mit AWS Organizations verwenden und keine Mitgliedskonten manuell eingeladen haben, gilt dieser Abschnitt nicht für Sie.

Ein Konto kann nicht gleichzeitig ein Administratorkonto und ein Mitgliedskonto sein.

Ein Mitgliedskonto kann nur einem Administratorkonto zugeordnet werden. Wenn ein Organisationskonto durch das Security Hub CSPM-Administratorkonto aktiviert wird, kann das Konto keine Einladung von einem anderen Konto annehmen. Wenn ein Konto bereits eine Einladung

akzeptiert hat, kann das Konto nicht durch das Security Hub CSPM-Administratorkonto für die Organisation aktiviert werden. Es kann auch keine Einladungen von anderen Konten empfangen.

Für den manuellen Einladungsprozess ist die Annahme einer Mitgliedschaftseinladung optional.

Mitgliedschaft durch AWS Organizations

Wenn Sie Security Hub CSPM mit integrieren AWS Organizations, kann das Verwaltungskonto der Organizations ein delegiertes Administratorkonto (DA) für Security Hub CSPM festlegen. Das Organisationsverwaltungskonto kann in Organizations nicht als DA festgelegt werden. Dies ist in Security Hub CSPM zwar zulässig, wir empfehlen jedoch, dass das Verwaltungskonto der Organizations nicht das DA sein sollte.

Wir empfehlen, dass Sie in allen Regionen dasselbe DA-Konto wählen. Wenn Sie die [zentrale Konfiguration](#) verwenden, richtet Security Hub CSPM in allen Regionen, in denen Sie Security Hub CSPM für Ihre Organisation konfigurieren, dasselbe DA-Konto ein.

Wir empfehlen außerdem, dass Sie für alle AWS Sicherheits- und Compliance-Dienste dasselbe DA-Konto wählen, damit Sie sicherheitsrelevante Probleme von einem zentralen Punkt aus verwalten können.

Mitgliedschaft auf Einladung

Bei Mitgliedskonten, die auf Einladung erstellt wurden, wird die Zuordnung zwischen Administrator und Mitgliedskonto nur in der Region erstellt, aus der die Einladung gesendet wurde. Das Administratorkonto muss Security Hub CSPM in jeder Region aktivieren, in der Sie es verwenden möchten. Das Administratorkonto lädt dann jedes Konto ein, ein Mitgliedskonto in dieser Region zu werden.

Note

Wir empfehlen, AWS Organizations anstelle von Security Hub CSPM-Einladungen zu verwenden, um Ihre Mitgliedskonten zu verwalten.

Koordination der Administratorkonten für alle Dienste

Security Hub CSPM fasst Ergebnisse verschiedener AWS Dienste wie Amazon GuardDuty, Amazon Inspector und Amazon Macie zusammen. Security Hub CSPM ermöglicht es Benutzern auch, von einem GuardDuty Ergebnis zu einer Untersuchung in Amazon Detective überzugehen.

Die Administrator-Mitglieds-Beziehungen, die Sie in diesen anderen Diensten einrichten, gelten jedoch nicht automatisch für Security Hub CSPM. Security Hub CSPM empfiehlt, dass Sie für all diese Dienste dasselbe Konto wie das Administratorkonto verwenden. Bei diesem Administratorkonto sollte es sich um ein Konto handeln, das für Sicherheitstools verantwortlich ist. Dasselbe Konto sollte auch das Aggregatorkonto für AWS Config sein.

Beispielsweise kann ein Benutzer des GuardDuty Administratorkontos A die Ergebnisse für die GuardDuty Mitgliedskonten B und C auf der GuardDuty Konsole sehen. Wenn Konto A dann Security Hub CSPM aktiviert, sehen Benutzer von Konto A nicht automatisch GuardDuty Ergebnisse für die Konten B und C in Security Hub CSPM. Für diese Konten ist auch eine Beziehung zwischen Security Hub CSPM-Administrator und Mitglied erforderlich.

Machen Sie dazu Konto A zum Security Hub CSPM-Administratorkonto und aktivieren Sie die Konten B und C, um Security Hub CSPM-Mitgliedskonten zu werden.

Security Hub CSPM für mehrere Konten verwalten mit AWS Organizations

Sie können AWS Security Hub Cloud Security Posture Management (CSPM) in Ihr Unternehmen integrieren und anschließend Security Hub CSPM für Konten in Ihrer Organisation verwalten. AWS Organizations

Um Security Hub CSPM zu integrieren AWS Organizations, erstellen Sie eine Organisation in. AWS Organizations Das Organisationsverwaltungs-konto bestimmt ein Konto als delegierten Security Hub CSPM-Administrator für die Organisation. Der delegierte Administrator kann dann Security Hub CSPM für andere Konten in der Organisation aktivieren, diese Konten als Security Hub CSPM-Mitgliedskonten hinzufügen und zulässige Aktionen für die Mitgliedskonten ausführen. Der delegierte Security Hub CSPM-Administrator kann Security Hub CSPM für bis zu 10.000 Mitgliedskonten aktivieren und verwalten.

[Der Umfang der Konfigurationsmöglichkeiten des delegierten Administrators hängt davon ab, ob Sie die zentrale Konfiguration verwenden.](#) Wenn die zentrale Konfiguration aktiviert ist, müssen Sie Security Hub CSPM nicht in jedem Mitgliedskonto separat konfigurieren und. AWS-Region Der delegierte Administrator kann spezifische Security Hub CSPM-Einstellungen in bestimmten Mitgliedskonten und Organisationseinheiten (OUs) regionsübergreifend durchsetzen.

Das delegierte Security Hub-CSPM-Administratorkonto kann die folgenden Aktionen für Mitgliedskonten ausführen:

- Wenn Sie die zentrale Konfiguration verwenden, konfigurieren Sie Security Hub CSPM zentral für Mitgliedskonten und OUs erstellen Sie Security Hub CSPM-Konfigurationsrichtlinien. Konfigurationsrichtlinien können verwendet werden, um Security Hub CSPM zu aktivieren und zu deaktivieren, Standards zu aktivieren und zu deaktivieren und Kontrollen zu aktivieren und zu deaktivieren.
- Behandeln Sie neue Konten automatisch als Security Hub CSPM-Mitgliedskonten, wenn sie der Organisation beitreten. Wenn Sie die zentrale Konfiguration verwenden, umfasst eine Konfigurationsrichtlinie, die einer Organisationseinheit zugeordnet ist, bestehende und neue Konten, die Teil der Organisationseinheit sind.
- Behandeln Sie bestehende Organisationskonten als Security Hub CSPM-Mitgliedskonten. Dies geschieht automatisch, wenn Sie die zentrale Konfiguration verwenden.
- Trennen Sie die Zuordnung von Mitgliedskonten, die zur Organisation gehören. Wenn Sie die zentrale Konfiguration verwenden, können Sie die Zuordnung eines Mitgliedskontos erst aufheben, nachdem Sie es als selbstverwaltet gekennzeichnet haben. Alternativ können Sie eine Konfigurationsrichtlinie, die Security Hub CSPM deaktiviert, bestimmten zentral verwalteten Mitgliedskonten zuordnen.

Wenn Sie sich nicht für die zentrale Konfiguration entscheiden, verwendet Ihr Unternehmen den Standardkonfigurationstyp, die als lokale Konfiguration bezeichnet wird. Bei der lokalen Konfiguration hat der delegierte Administrator eine eingeschränkere Möglichkeit, Einstellungen in Mitgliedskonten durchzusetzen. Weitere Informationen finden Sie unter [Grundlegendes zur lokalen Konfiguration in Security Hub CSPM](#).

Eine vollständige Liste der Aktionen, die der delegierte Administrator an Mitgliedskonten ausführen kann, finden Sie unter [Zulässige Aktionen von Administrator- und Mitgliedskonten in Security Hub CSPM](#)

In den Themen dieses Abschnitts wird erklärt, wie Security Hub CSPM in Security Hub CSPM für Konten in einer Organisation integriert AWS Organizations und verwaltet wird. Wo relevant, werden in jedem Abschnitt die Verwaltungsvorteile und Unterschiede für Benutzer der zentralen Konfiguration aufgeführt.

Themen

- [Integration von Security Hub CSPM mit AWS Organizations](#)
- [Automatisches Aktivieren von Security Hub CSPM in neuen Organisationskonten](#)
- [Manuelles Aktivieren von Security Hub CSPM in neuen Organisationskonten](#)

- [Trennung der Security Hub CSPM-Mitgliedskonten von Ihrer Organisation](#)

Integration von Security Hub CSPM mit AWS Organizations

Um AWS Security Hub Cloud Security Posture Management (CSPM) zu integrieren und AWS Organizations, erstellen Sie eine Organisation in Organizations und verwenden das Organisationsverwaltungskonto, um ein delegiertes Security Hub CSPM-Administratorkonto festzulegen. Dadurch wird Security Hub CSPM als vertrauenswürdiger Dienst in Organizations aktiviert. [Es aktiviert auch Security Hub CSPM in der aktuellen Version AWS-Region für das delegierte Administratorkonto und ermöglicht es dem delegierten Administrator, Security Hub CSPM für Mitgliedskonten zu aktivieren, Daten in Mitgliedskonten anzuzeigen und andere zulässige Aktionen für Mitgliedskonten durchzuführen.](#)

Wenn Sie die [zentrale Konfiguration](#) verwenden, kann der delegierte Administrator auch Security Hub CSPM-Konfigurationsrichtlinien erstellen, die angeben, wie der Security Hub CSPM-Dienst, die Standards und Kontrollen in Organisationskonten konfiguriert werden sollen.

Erstellen einer Organisation

Eine Organisation ist eine Entität, die Sie erstellen, um Ihre Organisation zu konsolidieren, AWS-Konten sodass Sie sie als eine Einheit verwalten können.

Sie können eine Organisation entweder mithilfe der AWS Organizations Konsole oder mithilfe eines Befehls aus dem SDK AWS CLI APIs oder einem der SDKs erstellen. Ausführliche Anweisungen finden [Sie im AWS Organizations Benutzerhandbuch unter Organisation erstellen.](#)

Sie können AWS Organizations damit alle Konten in Ihrer Organisation zentral anzeigen und verwalten. Eine Organisation besteht aus einem Verwaltungskonto und gegebenenfalls Mitgliedskonten. Sie können die Konten in einer hierarchischen, baumähnlichen Struktur mit einem Stamm an der Spitze und Organisationseinheiten (OUs) unter dem Stamm organisieren. Jedes Konto kann sich direkt unter dem Stamm befinden oder einem der Konten in der OUs Hierarchie zugeordnet werden. Eine OU ist ein Container für bestimmte Konten. Sie können beispielsweise eine Organisationseinheit für Finanzen erstellen, die alle Konten im Zusammenhang mit Finanzoperationen umfasst.

Empfehlungen für die Auswahl des delegierten Security Hub CSPM-Administrators

Wenn Sie über ein Administratorkonto aus dem manuellen Einladungsprozess verfügen und zur Kontoverwaltung mit wechseln, empfehlen wir AWS Organizations, dieses Konto als delegierten Security Hub CSPM-Administrator festzulegen.

Obwohl das Security Hub CSPM APIs und die Konsole es dem Organisationsverwaltungskonto ermöglichen, der delegierte Security Hub CSPM-Administrator zu sein, empfehlen wir, zwei verschiedene Konten zu wählen. Dies liegt daran, dass Benutzer, die Zugriff auf das Organisationsverwaltungskonto haben, um die Abrechnung zu verwalten, sich wahrscheinlich von Benutzern unterscheiden, die für die Sicherheitsverwaltung Zugriff auf Security Hub CSPM benötigen.

Wir empfehlen, in allen Regionen denselben delegierten Administrator zu verwenden. Wenn Sie sich für die zentrale Konfiguration entscheiden, benennt Security Hub CSPM automatisch denselben delegierten Administrator in Ihrer Heimatregion und allen verknüpften Regionen.

Überprüfen Sie die Berechtigungen zur Konfiguration des delegierten Administrators

Um ein delegiertes Security Hub CSPM-Administratorkonto zuzuweisen und zu entfernen, muss das Organisationsverwaltungskonto über Berechtigungen für die `DisableOrganizationAdminAccount` Aktionen `EnableOrganizationAdminAccount` und in Security Hub CSPM verfügen. Das Verwaltungskonto für Organizations muss auch über Administratorberechtigungen für Organizations verfügen.

Um alle erforderlichen Berechtigungen zu gewähren, fügen Sie dem IAM-Prinzipal für das Organisationsverwaltungskonto die folgenden von Security Hub verwalteten CSPM-Richtlinien hinzu:

- [AWSSecurityHubFullAccess](#)
- [AWSSecurityHubOrganizationsAccess](#)

Benennen des delegierten Administrators

Um das delegierte Security Hub CSPM-Administratorkonto festzulegen, können Sie die Security Hub CSPM-Konsole, die Security Hub CSPM-API oder verwenden. AWS CLI Security Hub CSPM legt den delegierten Administrator AWS-Region nur in der aktuellen Region fest, und Sie müssen die Aktion in anderen Regionen wiederholen. Wenn Sie die zentrale Konfiguration verwenden, richtet Security Hub CSPM automatisch denselben delegierten Administrator in der Heimatregion und den verknüpften Regionen ein.

Das Organisationsverwaltungskonto muss Security Hub CSPM nicht aktivieren, um das delegierte Security Hub CSPM-Administratorkonto zu bestimmen.

Wir empfehlen, dass das Organisationsverwaltungskonto nicht das delegierte Security Hub CSPM-Administratorkonto ist. Wenn Sie jedoch das Organisationsverwaltungskonto als delegierten Security Hub CSPM-Administrator wählen, muss Security Hub CSPM für das Verwaltungskonto aktiviert sein. Wenn Security Hub CSPM für das Verwaltungskonto nicht aktiviert ist, müssen Sie Security Hub CSPM manuell dafür aktivieren. Security Hub CSPM kann nicht automatisch für das Organisationsverwaltungskonto aktiviert werden.

Sie müssen den delegierten Security Hub CSPM-Administrator mit einer der folgenden Methoden benennen. Die Benennung des delegierten Security Hub CSPM-Administrators mit Organizations spiegelt APIs sich nicht in Security Hub CSPM wider.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten zur Benennung des delegierten Security Hub CSPM-Administratorkontos.

Security Hub CSPM console

Um den delegierten Administrator beim Onboarding zu bestimmen

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie Gehe zu Security Hub CSPM. Sie werden aufgefordert, sich mit dem Organisationsverwaltungskonto anzumelden.
3. Geben Sie auf der Seite Delegierten Administrator benennen im Abschnitt Delegiertes Administratorkonto das delegierte Administratorkonto an. Wir empfehlen, denselben delegierten Administrator zu wählen, den Sie für andere AWS Sicherheits- und Compliance-Dienste eingerichtet haben.
4. Wählen Sie Als delegierten Administrator festlegen aus. Sie werden aufgefordert, sich mit dem delegierten Administratorkonto anzumelden (falls Sie dies noch nicht getan haben), um das Onboarding mit der zentralen Konfiguration fortzusetzen. Wenn Sie die zentrale Konfiguration nicht starten möchten, wählen Sie Abbrechen. Ihr delegierter Administrator ist eingerichtet, aber Sie verwenden die zentrale Konfiguration noch nicht.

Um den delegierten Administrator auf der Seite „Einstellungen“ zu bestimmen

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Security Hub CSPM-Navigationsbereich die Option Einstellungen aus. Wählen Sie dann Allgemein.
3. Wenn derzeit ein Security Hub CSPM-Administratorkonto zugewiesen ist, müssen Sie das aktuelle Konto entfernen, bevor Sie ein neues Konto einrichten können.

Um das aktuelle Konto zu entfernen, wählen Sie unter Delegierter Administrator die Option Entfernen aus.

4. Geben Sie die Konto-ID des Kontos ein, das Sie als Security Hub CSPM-Administratorkonto festlegen möchten.

Sie müssen in allen Regionen dasselbe Security Hub CSPM-Administratorkonto angeben. Wenn Sie ein Konto angeben, das sich von dem in anderen Regionen angegebenen Konto unterscheidet, gibt die Konsole einen Fehler zurück.

5. Wählen Sie Delegieren.

Security Hub CSPM API, AWS CLI

Verwenden Sie vom Organisationsverwaltungskonto aus den [EnableOrganizationAdminAccount](#) Betrieb der Security Hub CSPM-API. Wenn Sie den verwenden AWS CLI, führen Sie den [enable-organization-admin-account](#) Befehl aus. Geben Sie die AWS-Konto ID des delegierten Security Hub CSPM-Administrators an.

Im folgenden Beispiel wird der delegierte Security Hub CSPM-Administrator benannt. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub enable-organization-admin-account --admin-account-id 123456789012
```

Den delegierten Administrator entfernen oder ändern

Nur das Organisationsverwaltungskonto kann das delegierte Security Hub CSPM-Administratorkonto entfernen.

Um den delegierten Security Hub CSPM-Administrator zu ändern, müssen Sie zuerst das aktuelle delegierte Administratorkonto entfernen und dann ein neues festlegen.

 Warning

Wenn Sie die [zentrale Konfiguration](#) verwenden, können Sie die Security Hub CSPM-Konsole oder Security Hub CSPM nicht verwenden, um das delegierte Administratorkonto APIs zu ändern oder zu entfernen. Wenn das Organisationsverwaltungskonto die AWS Organizations Konsole verwendet oder AWS Organizations APIs um den delegierten Security Hub CSPM-Administrator zu ändern oder zu entfernen, stoppt Security Hub CSPM automatisch die zentrale Konfiguration und löscht Ihre Konfigurationsrichtlinien und Richtlinienzuordnungen. Mitgliedskonten behalten die Konfigurationen bei, die sie hatten, bevor der delegierte Administrator geändert oder entfernt wurde.

Wenn Sie die Security Hub CSPM-Konsole verwenden, um den delegierten Administrator in einer Region zu entfernen, wird er automatisch in allen Regionen entfernt.

Die Security Hub CSPM API entfernt nur das delegierte Security Hub CSPM-Administratorkonto aus der Region, in der der API-Aufruf oder -Befehl ausgeführt wird. Sie müssen die Aktion in anderen Regionen wiederholen.

Wenn Sie das delegierte Security Hub CSPM-Administratorkonto mit der Organizations-API entfernen, wird es automatisch in allen Regionen entfernt.

Den delegierten Administrator entfernen (Organizations API, AWS CLI)

Sie können Organizations verwenden, um den delegierten Security Hub CSPM-Administrator in allen Regionen zu entfernen.

Wenn Sie die zentrale Konfiguration zur Verwaltung von Konten verwenden, führt das Entfernen des delegierten Administratorkontos dazu, dass Ihre Konfigurationsrichtlinien und Richtlinienverknüpfungen gelöscht werden. Mitgliedskonten behalten die Konfigurationen bei, die sie hatten, bevor der delegierte Administrator geändert oder entfernt wurde. Diese Konten können jedoch nicht mehr mit dem entfernten delegierten Administratorkonto verwaltet werden. Sie werden zu selbstverwalteten Konten, die in jeder Region separat konfiguriert werden müssen.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Anweisungen, um das delegierte Security Hub CSPM-Administratorkonto mit zu entfernen. AWS Organizations

Organizations API, AWS CLI

So entfernen Sie den delegierten Security Hub CSPM-Administrator

Verwenden Sie vom Organisationsverwaltungskonto aus den [DeregisterDelegatedAdministrator](#) Betrieb der Organisations-API. Wenn Sie den verwenden AWS CLI, führen Sie den [deregister-delegated-administrator](#) Befehl aus. Geben Sie die Konto-ID des delegierten Administrators und den Dienstprinzipal für Security Hub CSPM an, nämlich. `securityhub.amazonaws.com`

Im folgenden Beispiel wird der delegierte Security Hub CSPM-Administrator entfernt. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws organizations deregister-delegated-administrator --account-id 123456789012 --service-principal securityhub.amazonaws.com
```

Den delegierten Administrator entfernen (Security Hub CSPM-Konsole)

Sie können die Security Hub CSPM-Konsole verwenden, um den delegierten Security Hub CSPM-Administrator in allen Regionen zu entfernen.

Wenn das delegierte Security Hub CSPM-Administratorkonto entfernt wird, werden die Mitgliedskonten vom entfernten delegierten Security Hub CSPM-Administratorkonto getrennt.

Security Hub CSPM ist weiterhin in den Mitgliedskonten aktiviert. Sie werden zu eigenständigen Konten, bis ein neuer Security Hub CSPM-Administrator sie als Mitgliedskonten aktiviert.

Wenn das Organisationsverwaltungskonto kein aktiviertes Konto in Security Hub CSPM ist, verwenden Sie die Option auf der Seite Willkommen bei Security Hub CSPM.

So entfernen Sie das delegierte Security Hub CSPM-Administratorkonto von der Seite Willkommen bei Security Hub CSPM

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie Gehe zu Security Hub.
3. Wählen Sie unter Delegierter Administrator die Option Entfernen aus.

Wenn das Organisationsverwaltungskonto ein aktiviertes Konto in Security Hub ist, verwenden Sie die Option auf der Registerkarte Allgemein der Seite Einstellungen.

So entfernen Sie das delegierte Security Hub CSPM-Administratorkonto von der Seite Einstellungen

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Security Hub CSPM-Navigationsbereich die Option Einstellungen aus. Wählen Sie dann Allgemein.
3. Wählen Sie unter Delegierter Administrator die Option Entfernen aus.

Den delegierten Administrator entfernen (Security Hub CSPM API,) AWS CLI

Sie können die Security Hub CSPM-API oder die Security Hub CSPM-Operationen verwenden, AWS CLI um den delegierten Security Hub CSPM-Administrator zu entfernen. Wenn Sie den delegierten Administrator mit einer dieser Methoden entfernen, wird er nur in der Region entfernt, in der der API-Aufruf oder -Befehl ausgeführt wurde. Security Hub CSPM aktualisiert keine anderen Regionen und entfernt auch nicht das delegierte Administratorkonto in. AWS Organizations

Wählen Sie Ihre bevorzugte Methode und gehen Sie wie folgt vor, um das delegierte Security Hub CSPM-Administratorkonto bei Security Hub CSPM zu entfernen.

Security Hub CSPM API, AWS CLI

So entfernen Sie den delegierten Security Hub CSPM-Administrator

Verwenden Sie vom Organisationsverwaltungskonto aus den [DisableOrganizationAdminAccount](#) Betrieb der Security Hub CSPM-API. Wenn Sie den verwenden AWS CLI, führen Sie den [disable-organization-admin-account](#) Befehl aus. Geben Sie die Konto-ID des delegierten Security Hub CSPM-Administrators an.

Im folgenden Beispiel wird der delegierte Security Hub CSPM-Administrator entfernt. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub disable-organization-admin-account --admin-account-id 123456789012
```


Deaktivieren der Security Hub CSPM-Integration mit AWS Organizations

Nachdem eine AWS Organizations Organisation in AWS Security Hub Cloud Security Posture Management (CSPM) integriert wurde, kann das Verwaltungskonto der Organizations die Integration anschließend deaktivieren. Als Benutzer des Organisationsverwaltungskontos können Sie dies tun, indem Sie den vertrauenswürdigen Zugriff für Security Hub CSPM in deaktivieren. AWS Organizations

Wenn Sie den vertrauenswürdigen Zugriff für Security Hub CSPM deaktivieren, passiert Folgendes:

- Security Hub CSPM verliert seinen Status als vertrauenswürdiger Dienst in. AWS Organizations
- Das delegierte Security Hub CSPM-Administratorkonto verliert den Zugriff auf Security Hub CSPM-Einstellungen, Daten und Ressourcen für alle Security Hub CSPM-Mitgliedskonten insgesamt. AWS-Regionen
- Wenn Sie die [zentrale Konfiguration](#) verwendet haben, verwendet Security Hub CSPM sie automatisch nicht mehr für Ihr Unternehmen. Ihre Konfigurationsrichtlinien und Richtlinienverknüpfungen werden gelöscht. Konten behalten die Konfigurationen bei, die sie hatten, bevor Sie den vertrauenswürdigen Zugriff deaktiviert haben.
- Alle Security Hub CSPM-Mitgliedskonten werden zu eigenständigen Konten und behalten ihre aktuellen Einstellungen bei. Wenn Security Hub CSPM für ein Mitgliedskonto in einer oder mehreren Regionen aktiviert wurde, ist Security Hub CSPM weiterhin für das Konto in diesen Regionen aktiviert. Die aktivierten Standards und Kontrollen bleiben ebenfalls unverändert. Sie können diese Einstellungen für jedes Konto und jede Region separat ändern. Das Konto ist jedoch in keiner Region mehr einem delegierten Administrator zugeordnet.

Weitere Informationen zu den Ergebnissen der Deaktivierung des Zugriffs auf vertrauenswürdige Dienste finden Sie AWS-Services im AWS Organizations Benutzerhandbuch [unter AWS Organizations Zusammen mit anderen Benutzern verwenden](#).

Um den vertrauenswürdigen Zugriff zu deaktivieren, können Sie die AWS Organizations Konsole, die Organisations-API oder die verwenden AWS CLI. Nur ein Benutzer des Organisationsverwaltungskontos kann den vertrauenswürdigen Dienstzugriff für Security Hub CSPM deaktivieren. Einzelheiten zu den Berechtigungen, die Sie benötigen, finden Sie im AWS Organizations Benutzerhandbuch unter [Erforderliche Berechtigungen zur Deaktivierung des vertrauenswürdigen Zugriffs](#).

Bevor Sie den vertrauenswürdigen Zugriff deaktivieren, empfehlen wir, mit dem delegierten Administrator Ihrer Organisation zusammenzuarbeiten, um Security Hub CSPM in Mitgliedskonten zu deaktivieren und die Security Hub CSPM-Ressourcen in diesen Konten zu bereinigen.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um den vertrauenswürdigen Zugriff für Security Hub CSPM zu deaktivieren.

Organizations console

So deaktivieren Sie den vertrauenswürdigen Zugriff für Security Hub CSPM

1. Melden Sie sich AWS Management Console mit den Anmeldeinformationen des AWS Organizations Verwaltungskontos an.
2. Öffnen Sie die Organisationskonsole unter <https://console.aws.amazon.com/organizations/>.
3. Wählen Sie im Navigationsbereich Services.
4. Wählen Sie unter Integrierte Dienste die Option AWS Security Hub Cloud Security Posture Management (CSPM) aus.
5. Wählen Sie Vertrauenswürdigen Zugriff deaktivieren.
6. Bestätigen Sie, dass Sie den vertrauenswürdigen Zugriff deaktivieren möchten.

Organizations API

So deaktivieren Sie den vertrauenswürdigen Zugriff für Security Hub CSPM

Rufen [Sie den Vorgang „AWSServiceZugriff deaktivieren“ der API auf](#). AWS Organizations Geben Sie für den ServicePrincipal Parameter den Security Hub CSPM-Dienstprinzipal () `securityhub.amazonaws.com` an.

AWS CLI

So deaktivieren Sie den vertrauenswürdigen Zugriff für Security Hub CSPM

Führen Sie den [disable-aws-service-access](#) Befehl der API aus. AWS Organizations Geben Sie für den service-principal Parameter den Security Hub CSPM-Dienstprinzipal () `securityhub.amazonaws.com` an.

Beispiel:

```
aws organizations disable-aws-service-access --service-principal
securityhub.amazonaws.com
```

Automatisches Aktivieren von Security Hub CSPM in neuen Organisationskonten

Wenn neue Konten Ihrer Organisation beitreten, werden sie der Liste auf der Kontoseite der AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole hinzugefügt. Für Organisationskonten lautet Typ auf Nach Organisation. Standardmäßig werden neue Konten nicht zu Security Hub CSPM-Mitgliedern, wenn sie der Organisation beitreten. Ihr Status ist Kein Mitglied. Das delegierte Administratorkonto kann automatisch neue Konten als Mitglieder hinzufügen und Security Hub CSPM in diesen Konten aktivieren, wenn sie der Organisation beitreten.

Note

Obwohl viele Regionen standardmäßig für Sie aktiv AWS-Regionen sind AWS-Konto, müssen Sie bestimmte Regionen manuell aktivieren. Diese Regionen werden in diesem Dokument als Opt-in-Regionen bezeichnet. Um Security Hub CSPM automatisch in einem neuen Konto in einer Opt-in-Region zu aktivieren, muss diese Region zuerst für das Konto aktiviert sein. Nur der Kontoinhaber kann die Opt-in-Region aktivieren. Weitere Informationen zu Opt-in-Regionen findest du unter [Geben Sie an, welche Regionen für AWS-Regionen Ihr Konto verwendet werden können](#).

Dieser Vorgang unterscheidet sich je nachdem, ob Sie die zentrale Konfiguration (empfohlen) oder die lokale Konfiguration verwenden.

Automatische Aktivierung neuer Organisationskonten (zentrale Konfiguration)

Wenn Sie die [zentrale Konfiguration](#) verwenden, können Sie Security Hub CSPM automatisch in neuen und bestehenden Organisationskonten aktivieren, indem Sie eine Konfigurationsrichtlinie erstellen, in der Security Hub CSPM aktiviert ist. Anschließend können Sie die Richtlinie dem Organisationsstamm oder bestimmten Organisationseinheiten zuordnen (). OUs

Wenn Sie eine Konfigurationsrichtlinie, in der Security Hub CSPM aktiviert ist, einer bestimmten OU zuordnen, wird Security Hub CSPM automatisch in allen Konten (vorhandenen und neuen) aktiviert, die zu dieser OU gehören. Neue Konten, die nicht zur Organisationseinheit gehören, werden selbst verwaltet und Security Hub CSPM ist nicht automatisch aktiviert. Wenn Sie dem Root eine Konfigurationsrichtlinie zuordnen, in der Security Hub CSPM aktiviert ist, wird Security Hub CSPM automatisch in allen Konten (vorhandenen und neuen) aktiviert, die der Organisation beitreten.

Ausnahmen sind, wenn ein Konto aufgrund von Anwendung oder Vererbung eine andere Richtlinie verwendet oder wenn es sich um ein selbstverwaltetes Konto handelt.

In Ihrer Konfigurationsrichtlinie können Sie auch definieren, welche Sicherheitsstandards und Kontrollen in der Organisationseinheit aktiviert werden sollen. Um Kontrollergebnisse für aktivierte Standards zu generieren, müssen die Konten in der Organisationseinheit AWS Config aktiviert und konfiguriert sein, um die erforderlichen Ressourcen aufzuzeichnen. Weitere Informationen zur AWS Config Aufzeichnung finden Sie unter [Aktivieren und Konfigurieren AWS Config](#).

Anweisungen zum Erstellen einer Konfigurationsrichtlinie finden Sie unter [Konfigurationsrichtlinien erstellen und zuordnen](#).

Automatisches Aktivieren neuer Organisationskonten (lokale Konfiguration)

Wenn Sie die lokale Konfiguration verwenden und die automatische Aktivierung von Standardstandards aktivieren, fügt Security Hub CSPM neue Organisationskonten als Mitglieder hinzu und aktiviert Security Hub CSPM in diesen Konten in der aktuellen Region. Andere Regionen sind nicht betroffen. Darüber hinaus aktiviert die Aktivierung der automatischen Aktivierung Security Hub CSPM nicht in bestehenden Organisationskonten, es sei denn, sie wurden bereits als Mitgliedskonten hinzugefügt.

Nach der Aktivierung der automatischen Aktivierung werden die Standardsicherheitsstandards für neue Mitgliedskonten in der aktuellen Region aktiviert, wenn sie der Organisation beitreten. Die Standardstandards sind AWS Foundational Security Best Practices (FSBP) und Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. Sie können die Standardstandards nicht ändern. Wenn Sie andere Standards in Ihrer Organisation aktivieren oder Standards für ausgewählte Konten aktivieren möchten OUs, empfehlen wir die zentrale Konfiguration.

Um Kontrollergebnisse für die Standardstandards (und andere aktivierte Standards) zu generieren, müssen die Konten in Ihrer Organisation AWS Config aktiviert und konfiguriert sein, um die erforderlichen Ressourcen aufzuzeichnen. Weitere Informationen zur AWS Config Aufzeichnung finden Sie unter [Aktivieren und Konfigurieren AWS Config](#).

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um Security Hub CSPM automatisch in neuen Unternehmenskonten zu aktivieren. Diese Anweisungen gelten nur, wenn Sie die lokale Konfiguration verwenden.

Security Hub CSPM console

So aktivieren Sie automatisch neue Organisationskonten als Security Hub CSPM-Mitglieder

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>

Sign verwendet die Anmeldeinformationen des delegierten Administratorkontos.

2. Wählen Sie im Security Hub CSPM-Navigationsbereich unter Einstellungen die Option Konfiguration aus.
3. Aktivieren Sie im Abschnitt Konten die Option Konten automatisch aktivieren.

Security Hub CSPM API

So aktivieren Sie automatisch neue Organisationskonten als Security Hub CSPM-Mitglieder

Rufen Sie die [UpdateOrganizationConfiguration](#)API vom delegierten Administratorkonto aus auf. Stellen Sie das AutoEnable Feld auf ein `true`, um Security Hub CSPM automatisch in neuen Organisationskonten zu aktivieren.

AWS CLI

So aktivieren Sie automatisch neue Organisationskonten als Security Hub CSPM-Mitglieder

Führen Sie den [update-organization-configuration](#)Befehl über das delegierte Administratorkonto aus. Fügen Sie den `auto-enable` Parameter hinzu, um Security Hub CSPM automatisch in neuen Organisationskonten zu aktivieren.

```
aws securityhub update-organization-configuration --auto-enable
```

Manuelles Aktivieren von Security Hub CSPM in neuen Organisationskonten

Wenn Sie Security Hub CSPM nicht automatisch in neuen Organisationskonten aktivieren, wenn diese der Organisation beitreten, können Sie diese Konten als Mitglieder hinzufügen und Security Hub CSPM in ihnen manuell aktivieren, nachdem sie der Organisation beigetreten sind. Sie müssen Security Hub CSPM auch manuell aktivieren, da Sie zuvor AWS-Konten die Verbindung zu einer Organisation getrennt haben.

 Note

Dieser Abschnitt gilt nicht für Sie, wenn Sie die zentrale Konfiguration verwenden. Wenn Sie die zentrale Konfiguration verwenden, können Sie Konfigurationsrichtlinien erstellen, die Security Hub CSPM in bestimmten Mitgliedskonten und Organisationseinheiten aktivieren (OUs). Sie können auch spezifische Standards und Kontrollen für diese Konten und aktivieren. OUs

Sie können Security Hub CSPM nicht in einem Konto aktivieren, wenn es sich bereits um ein Mitgliedskonto in einer anderen Organisation handelt.

Sie können Security Hub CSPM auch nicht in einem Konto aktivieren, das derzeit gesperrt ist. Wenn Sie versuchen, den Dienst in einem gesperrten Konto zu aktivieren, ändert sich der Kontostatus in Konto gesperrt.

- Wenn Security Hub CSPM für das Konto nicht aktiviert ist, ist Security Hub CSPM in diesem Konto aktiviert. Der Standard AWS Foundational Security Best Practices (FSBP) und der CIS AWS Foundations Benchmark v1.2.0 sind ebenfalls im Konto aktiviert, sofern Sie die Standardsicherheitsstandards nicht deaktivieren.

Eine Ausnahme bildet das Verwaltungskonto für Organizations. Security Hub CSPM kann nicht automatisch im Verwaltungskonto der Organizations aktiviert werden. Sie müssen Security Hub CSPM manuell im Verwaltungskonto der Organizations aktivieren, bevor Sie es als Mitgliedskonto hinzufügen können.

- Wenn Security Hub CSPM für das Konto bereits aktiviert ist, nimmt Security Hub CSPM keine weiteren Änderungen am Konto vor. Es aktiviert nur die Mitgliedschaft.

Damit Security Hub CSPM Kontrollergebnisse generieren kann, müssen Mitgliedskonten AWS Config aktiviert und konfiguriert sein, um die erforderlichen Ressourcen aufzuzeichnen. Weitere Informationen zur Konfiguration von SSH finden Sie unter [Aktivieren und Konfigurieren von AWS Config](#).

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um ein Organisationskonto als Security Hub CSPM-Mitgliedskonto zu aktivieren.

Security Hub CSPM console

Um Organisationskonten manuell als Security Hub CSPM-Mitglieder zu aktivieren

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>

Melden Sie sich mit den Anmeldeinformationen des delegierten Administratorkontos an.

2. Wählen Sie im Security Hub CSPM-Navigationsbereich unter Einstellungen die Option Konfiguration aus.
3. Wählen Sie in der Kontenliste jedes Unternehmenskonto aus, das Sie aktivieren möchten.
4. Wählen Sie Aktionen und dann Mitglied hinzufügen aus.

Security Hub CSPM API

Um Organisationskonten manuell als Security Hub CSPM-Mitglieder zu aktivieren

Rufen Sie die [CreateMembers](#) API vom delegierten Administratorkonto aus auf. Geben Sie für jedes Konto, das aktiviert werden soll, die Konto-ID an.

Im Gegensatz zum manuellen Einladungsprozess müssen `CreateMembers` Sie bei der Aktivierung eines Unternehmenskontos keine Einladung versenden.

AWS CLI

Um Organisationskonten manuell als Security Hub CSPM-Mitglieder zu aktivieren

Führen Sie den [create-members](#) Befehl über das delegierte Administratorkonto aus. Geben Sie für jedes Konto, das aktiviert werden soll, die Konto-ID an.

Im Gegensatz zum manuellen Einladungsprozess `create-members` müssen Sie bei der Aktivierung eines Unternehmenskontos keine Einladung versenden.

```
aws securityhub create-members --account-details '[{"AccountId": "<accountId>"}]'
```

Beispiel

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"}, {"AccountId": "123456789222"}]'
```

Trennung der Security Hub CSPM-Mitgliedskonten von Ihrer Organisation

Wenn Sie keine Ergebnisse von einem AWS Security Hub Cloud Security Posture Management (CSPM) -Mitgliedskonto mehr erhalten und ansehen möchten, können Sie das Mitgliedskonto von Ihrer Organisation trennen.

Note

Wenn Sie die [zentrale Konfiguration verwenden, funktioniert](#) die Trennung anders. Sie können eine Konfigurationsrichtlinie erstellen, die Security Hub CSPM in einem oder mehreren zentral verwalteten Mitgliedskonten deaktiviert. Danach sind diese Konten immer noch Teil der Organisation, generieren aber keine CSPM-Ergebnisse von Security Hub. Wenn Sie die zentrale Konfiguration verwenden, aber auch über manuell eingeladene Mitgliedskonten verfügen, können Sie die Zuordnung zu einem oder mehreren manuell eingeladenen Konten aufheben.

Mitgliedskonten, die über verwaltet werden, AWS Organizations können ihre Konten nicht vom Administratorkonto trennen. Nur das Administratorkonto kann die Zuordnung eines Mitgliedskontos aufheben.

Durch das Aufheben der Zuordnung zu einem Mitgliedskonto wird das Konto nicht geschlossen. Stattdessen wird das Mitgliedskonto aus der Organisation entfernt. Das getrennte Mitgliedskonto wird zu einem eigenständigen Konto AWS-Konto , das nicht mehr von der Security Hub CSPM-Integration mit verwaltet wird. AWS Organizations

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um ein Mitgliedskonto von der Organisation zu trennen.

Security Hub CSPM console

Um ein Mitgliedskonto von der Organisation zu trennen

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>

Melden Sie sich mit den Anmeldeinformationen des delegierten Administratorkontos an.

2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Konfiguration aus.

3. Wählen Sie im Abschnitt Konten die Konten aus, deren Verknüpfung Sie aufheben möchten. Wenn Sie die zentrale Konfiguration verwenden, können Sie auf der Registerkarte ein manuell eingerichtetes Konto auswählen, dessen Verbindung aufgehoben werden soll. **Invitation accounts** Diese Registerkarte ist nur sichtbar, wenn Sie die zentrale Konfiguration verwenden.
4. Wählen Sie Aktionen und anschließend Konto trennen aus.

Security Hub CSPM API

Um ein Mitgliedskonto von der Organisation zu trennen

Rufen Sie die [DisassociateMembers](#) API vom delegierten Administratorkonto aus auf. Sie müssen das angeben, damit die AWS-Konto IDs Mitgliedskonten die Verknüpfung aufheben können. Rufen Sie die API auf, um eine Liste der Mitgliedskonten anzuzeigen. [ListMembers](#)

AWS CLI

Um ein Mitgliedskonto von der Organisation zu trennen

Führen Sie den `disassociate-members` Befehl [≥](#) vom delegierten Administratorkonto aus. Sie müssen das angeben, damit die AWS-Konto IDs Mitgliedskonten die Verknüpfung aufheben können. Um eine Liste der Mitgliedskonten anzuzeigen, führen Sie den `list-members` Befehl [≥](#) aus.

```
aws securityhub disassociate-members --account-ids "<accountIds>"
```

Beispiel

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

Sie können auch die AWS Organizations Konsole oder verwenden AWS CLI, AWS SDKs um die Zuordnung eines Mitgliedskontos zu Ihrer Organisation aufzuheben. Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter [Entfernen eines Mitgliedskontos aus Ihrer Organisation](#).

Konten auf Einladung in Security Hub CSPM verwalten

Sie können mehrere AWS Security Hub Cloud Security Posture Management (CSPM) -Konten auf zwei Arten zentral verwalten: durch die Integration von Security Hub CSPM in AWS Organizations oder durch manuelles Senden und Akzeptieren von Mitgliedschaftseinladungen. Sie müssen den manuellen Prozess verwenden, wenn Sie ein eigenständiges Konto haben oder wenn Sie es nicht integrieren möchten. AWS Organizations Bei der manuellen Kontoverwaltung lädt der Security Hub CSPM-Administrator Konten ein, Mitglieder zu werden. Die Beziehung zwischen Administrator und Mitglied wird hergestellt, wenn ein potenzielles Mitglied die Einladung annimmt. Ein Security Hub CSPM-Administratorkonto kann Security Hub CSPM für bis zu 1.000 Mitgliedskonten verwalten, die auf Einladung basieren.

Note

Wenn Sie in Security Hub CSPM eine Organisation erstellen, die auf Einladung basiert, können Sie anschließend auf die Verwendung von CSPM [umsteigen](#). AWS Organizations Wenn Sie mehr als ein Mitgliedskonto haben, empfehlen wir, AWS Organizations anstelle von Security Hub CSPM-Einladungen zu verwenden, um Ihre Mitgliedskonten zu verwalten. Weitere Informationen finden Sie unter [Security Hub CSPM für mehrere Konten verwalten mit AWS Organizations](#).

Die regionsübergreifende Aggregation von Ergebnissen und anderen Daten ist für Konten verfügbar, die Sie über den manuellen Einladungsprozess einladen. Der Administrator muss jedoch das Mitgliedskonto aus der Aggregationsregion und allen verknüpften Regionen einladen, damit die regionsübergreifende Aggregation funktioniert. Darüber hinaus muss für das Mitgliedskonto Security Hub CSPM in der Aggregationsregion und allen verknüpften Regionen aktiviert sein, damit der Administrator die Ergebnisse des Mitgliedskontos einsehen kann.

Konfigurationsrichtlinien werden für manuell eingeladene Mitgliedskonten nicht unterstützt. Stattdessen müssen Sie die Security Hub CSPM-Einstellungen in jedem Mitgliedskonto und AWS-Region bei Verwendung des manuellen Einladungsprozesses separat konfigurieren.

Sie müssen den manuellen Einladungsprozess auch für Konten verwenden, die nicht zu Ihrer Organisation gehören. Beispielsweise könnten Sie in Ihrer Organisation kein Testkonto einrichten. Oder vielleicht möchten Sie Konten mehrerer Organisationen unter einem einzigen Security Hub CSPM-Administratorkonto konsolidieren. Das Security Hub CSPM-Administratorkonto muss Einladungen an Konten senden, die anderen Organisationen gehören.

Auf der Konfigurationsseite der Security Hub CSPM-Konsole werden Konten, die auf Einladung hinzugefügt wurden, auf der Registerkarte Einladungskonten aufgeführt. Wenn Sie die [zentrale Konfiguration](#) verwenden, aber auch Konten außerhalb Ihrer Organisation einladen, können Sie sich auf dieser Registerkarte die Ergebnisse von Konten ansehen, die auf Einladungen basieren. Der Security Hub CSPM-Administrator kann jedoch mithilfe von Konfigurationsrichtlinien keine Konten, die auf Einladungen basieren, regionsübergreifend konfigurieren.

In den Themen in diesem Abschnitt wird erklärt, wie Mitgliedskonten mithilfe von Einladungen verwaltet werden.

Themen

- [Mitgliedskonten in Security Hub CSPM hinzufügen und einladen](#)
- [Auf eine Einladung antworten, ein Security Hub CSPM-Mitgliedskonto zu werden](#)
- [Aufheben der Zuordnung von Mitgliedskonten in Security Hub CSPM](#)
- [Löschen von Mitgliedskonten in Security Hub CSPM](#)
- [Trennung von einem Security Hub CSPM-Administratorkonto](#)
- [Umstellung auf Organizations zur Verwaltung von Konten in Security Hub CSPM](#)

Mitgliedskonten in Security Hub CSPM hinzufügen und einladen

Note

Wir empfehlen, AWS Organizations anstelle von Security Hub CSPM-Einladungen zu verwenden, um Ihre Mitgliedskonten zu verwalten. Weitere Informationen finden Sie unter [Security Hub CSPM für mehrere Konten verwalten mit AWS Organizations](#).

Ihr Konto wird zum AWS Security Hub Cloud Security Posture Management (CSPM) -Administrator für Konten, die Ihre Einladung annehmen, ein Security Hub CSPM-Mitgliedskonto zu werden.

Wenn Sie eine Einladung von einem anderen Konto annehmen, wird Ihr Konto zu einem Mitgliedskonto und dieses Konto wird zu Ihrem Administrator.

Wenn es sich bei Ihrem Konto um ein Administratorkonto handelt, können Sie eine Einladung, ein Mitgliedskonto zu werden, nicht annehmen.

Das Hinzufügen eines Mitgliedskontos besteht aus den folgenden Schritten:

1. Das Administratorkonto fügt das Mitgliedskonto zu seiner Liste der Mitgliedskonten hinzu.
2. Das Administratorkonto sendet eine Einladung an das Mitgliedskonto.
3. Das Mitgliedskonto akzeptiert die Einladung.

Mitgliedskonten hinzufügen

Von der Security Hub CSPM-Konsole aus können Sie Konten zu Ihrer Liste der Mitgliedskonten hinzufügen. In der Security Hub CSPM-Konsole können Sie Konten einzeln auswählen oder eine .csv Datei hochladen, die die Kontoinformationen enthält.

Für jedes Konto müssen Sie die Konto-ID und eine E-Mail-Adresse angeben. Die E-Mail-Adresse sollte die E-Mail-Adresse sein, an die Sie sich bei Sicherheitsproblemen im Konto wenden können. Sie wird nicht zur Verifizierung des Kontos verwendet.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten zum Hinzufügen von Mitgliedskonten.

Security Hub CSPM console

Um Konten zu deiner Liste von Mitgliedskonten hinzuzufügen

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>

Melden Sie sich mit den Anmeldeinformationen des Administratorkontos an.

2. Wählen Sie im linken Bereich Settings (Einstellungen) aus.
3. Wählen Sie auf der Seite Einstellungen die Option Konten und dann Konten hinzufügen aus. Sie können dann entweder einzelne Konten hinzufügen oder eine .csv Datei hochladen, die die Liste der Konten enthält.
4. Gehen Sie wie folgt vor, um die Konten auszuwählen:
 - Um die Konten einzeln hinzuzufügen, geben Sie unter Konten eingeben die Konto-ID und die E-Mail-Adresse des hinzuzufügenden Kontos ein, und wählen Sie dann Hinzufügen aus.

Wiederholen Sie diesen Vorgang für jedes Konto.

- Um eine Datei mit kommagetrennten Werten (.csv) zum Hinzufügen mehrerer Konten zu verwenden, erstellen Sie zunächst die Datei. Die Datei muss die Konto-ID und die E-Mail-Adresse für jedes hinzuzufügende Konto enthalten.

In Ihrer .csv Liste muss eines pro Zeile erscheinen. Die erste Zeile der .csv Datei muss den Header enthalten. In der Kopfzeile befindet sich die erste Spalte **Account ID** und die zweite Spalte ist **Email**.

Jede weitere Zeile muss eine gültige Konto-ID und eine gültige E-Mail-Adresse für das Konto enthalten, das Sie hinzufügen möchten.

Hier ist ein Beispiel für eine .csv Datei, wenn sie in einem Texteditor angezeigt wird.

```
Account ID,Email
111111111111,user@example.com
```

In einem Tabellenkalkulationsprogramm werden die Felder in separaten Spalten angezeigt. Das zugrunde liegende Format ist immer noch durch Kommas getrennt. Sie müssen das Konto IDs als Zahlen ohne Dezimalzahlen formatieren. Beispielsweise kann die Konto-ID 444455556666 nicht als 444455556666.0 formatiert werden. Stellen Sie außerdem sicher, dass bei der Zahlenformatierung keine führenden Nullen aus der Konto-ID entfernt werden.

Um die Datei auszuwählen, wählen Sie auf der Konsole die Option Liste hochladen (.csv). Wählen Sie dann „Durchsuchen“.

Nachdem Sie die Datei ausgewählt haben, wählen Sie Konten hinzufügen.

5. Wenn Sie mit dem Hinzufügen von Konten fertig sind, wählen Sie unter Hinzuzufügende Konten die Option Weiter aus.

Security Hub CSPM API

Um Konten zu Ihrer Liste von Mitgliedskonten hinzuzufügen

Rufen Sie die [CreateMembers](#) API vom Administratorkonto aus auf. Für jedes Mitgliedskonto, das hinzugefügt werden soll, müssen Sie die AWS-Konto ID angeben.

AWS CLI

Um Konten zu Ihrer Liste von Mitgliedskonten hinzuzufügen

Führen Sie den [create-members](#) Befehl vom Administratorkonto aus. Für jedes Mitgliedskonto, das hinzugefügt werden soll, müssen Sie die AWS-Konto ID angeben.

```
aws securityhub create-members --account-details '[{"AccountId": "<accountID1>"}]'
```

Beispiel

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"}, {"AccountId": "123456789222"}]'
```

Mitgliedskonten einladen

Nachdem Sie die Mitgliedskonten hinzugefügt haben, senden Sie eine Einladung an das Mitgliedskonto. Sie können eine Einladung auch erneut an ein Konto senden, das Sie vom Administrator getrennt haben.

Security Hub CSPM console

Um Konten potenzieller Mitglieder einzuladen

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>

Melden Sie sich mit den Anmeldeinformationen des Administratorkontos an.

2. Wählen Sie im Navigationsbereich Einstellungen und dann Konten aus.
3. Wählen Sie für das einzuladende Konto Invite (Einladen) in der Spalte Status aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Einladen aus.

Note

Um Einladungen an getrennte Konten erneut zu senden, wählen Sie auf der Seite Konten jedes getrennte Konto aus. Wählen Sie unter Aktionen die Option Einladung erneut senden aus.

Security Hub CSPM API

Um Konten potenzieller Mitglieder einzuladen

Rufen Sie die [InviteMembers](#) API vom Administratorkonto aus auf. Für jedes Konto, das eingeladen werden soll, müssen Sie die AWS-Konto ID angeben.

AWS CLI

Um Konten potenzieller Mitglieder einzuladen

Führen Sie den [invite-members](#) Befehl vom Administratorkonto aus. Für jedes Konto, das eingeladen werden soll, müssen Sie die AWS-Konto ID angeben.

```
aws securityhub invite-members --account-ids <accountIDs>
```

Beispiel

```
aws securityhub invite-members --account-ids "123456789111" "123456789222"
```

Auf eine Einladung antworten, ein Security Hub CSPM-Mitgliedskonto zu werden

Note

Wir empfehlen, AWS Organizations anstelle von Security Hub CSPM-Einladungen zu verwenden, um Ihre Mitgliedskonten zu verwalten. Weitere Informationen finden Sie unter [Security Hub CSPM für mehrere Konten verwalten mit AWS Organizations](#).

Sie können eine Einladung, ein Mitgliedskonto für AWS Security Hub Cloud Security Posture Management (CSPM) zu werden, annehmen oder ablehnen.

Wenn Sie eine Einladung annehmen, wird Ihr Konto zu einem Security Hub CSPM-Mitgliedskonto. Das Konto, das die Einladung gesendet hat, wird zu Ihrem Security Hub CSPM-Administratorkonto. Der Benutzer des Administratorkontos kann die Ergebnisse für Ihr Mitgliedskonto in Security Hub CSPM einsehen.

Wenn Sie die Einladung ablehnen, wird Ihr Konto in der Liste der Mitgliedskonten des Administratorkontos als **Kündigt** markiert.

Sie können nur eine Einladung annehmen, ein Mitgliedskonto zu werden.

Bevor Sie eine Einladung annehmen oder ablehnen können, müssen Sie Security Hub CSPM aktivieren.

Denken Sie daran, dass alle Security Hub CSPM-Konten AWS Config aktiviert und konfiguriert sein müssen, um alle Ressourcen aufzuzeichnen. Einzelheiten zu den Anforderungen für finden Sie AWS Config unter [Aktivierung und Konfiguration](#). AWS Config

Eine Einladung annehmen

Sie können vom Administratorkonto aus eine Einladung senden, ein Security Hub CSPM-Mitgliedskonto zu werden. Sie können die Einladung dann annehmen, nachdem Sie sich mit dem Mitgliedskonto angemeldet haben.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um eine Einladung als Mitgliedskonto anzunehmen.

Security Hub CSPM console

Um eine Einladung zur Mitgliedschaft anzunehmen

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Einstellungen und dann Konten aus.
3. Aktivieren Sie im Abschnitt Administratorkonto die Option Annehmen und wählen Sie dann Einladung annehmen aus.

Security Hub CSPM API

Um eine Einladung zur Mitgliedschaft anzunehmen

Rufen Sie die [AcceptAdministratorInvitation](#)API auf. Sie müssen die Einladungs-ID und die AWS-Konto ID des Administratorkontos angeben. Verwenden Sie den [ListInvitations](#)Vorgang, um Details zur Einladung abzurufen.

AWS CLI

Um eine Einladung zur Mitgliedschaft anzunehmen

Führen Sie den Befehl [accept-administrator-invitation](#) aus. Sie müssen die Einladungs-ID und die AWS-Konto ID des Administratorkontos angeben. Führen Sie den [list-invitations](#)Befehl aus, um Details zur Einladung abzurufen.


```
aws securityhub accept-administrator-invitation --administrator-id <administratorAccountID> --invitation-id <invitationID>
```

Beispiel

```
aws securityhub accept-administrator-invitation --administrator-id 123456789012 --invitation-id 7ab938c5d52d7904ad09f9e7c20cc4eb
```

Note

Die Security Hub CSPM-Konsole wird weiterhin verwendet. `AcceptInvitation` Sie wird irgendwann auf `Verwendung` umgestellt. `AcceptAdministratorInvitation` Alle IAM-Richtlinien, die speziell den Zugriff auf diese Funktion regeln, müssen weiterhin verwendet `AcceptInvitation` werden. Sie sollten Ihre Richtlinien auch ergänzen `AcceptAdministratorInvitation`, um sicherzustellen, dass nach Beginn der Nutzung `AcceptAdministratorInvitation` der Konsole die richtigen Berechtigungen vorhanden sind.

Eine Einladung ablehnen

Sie können eine Einladung als Security Hub CSPM-Mitgliedskonto ablehnen. Wenn Sie eine Einladung in der Security Hub CSPM-Konsole ablehnen, wird Ihr Konto in der Liste der Mitgliedskonten des Administratorkontos als `Signiert` markiert. Der Status `Kündigt` wird nur angezeigt, wenn Sie sich mit dem Administratorkonto bei der Security Hub CSPM-Konsole anmelden. Die Einladung bleibt jedoch unverändert in der Konsole für das Mitgliedskonto, bis Sie sich beim Administratorkonto anmelden und die Einladung löschen.

Um eine Einladung abzulehnen, müssen Sie sich bei dem Mitgliedskonto anmelden, das die Einladung erhalten hat.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um eine Einladung als Mitgliedskonto abzulehnen.

Security Hub CSPM console

Um eine Einladung zur Mitgliedschaft abzulehnen

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Einstellungen und dann Konten aus.
3. Wählen Sie im Abschnitt Administratorkonto die Option Einladung ablehnen aus.

Security Hub CSPM API

Um eine Einladung zur Mitgliedschaft abzulehnen

Rufen Sie die [DeclineInvitations](#) API auf. Sie müssen die AWS-Konto ID des Administratorkontos angeben, das die Einladung ausgestellt hat. Verwenden Sie den [ListInvitations](#) Vorgang, um Informationen zu Ihren Einladungen anzuzeigen.

AWS CLI

Um eine Einladung zur Mitgliedschaft abzulehnen

Führen Sie den Befehl [decline-invitations](#) aus. Sie müssen die AWS-Konto ID des Administratorkontos angeben, das die Einladung ausgestellt hat. Führen Sie den [list-invitations](#) Befehl aus, um Informationen zu Ihren Einladungen anzuzeigen.

```
aws securityhub decline-invitations --account-ids "<administratorAccountId>"
```

Beispiel

```
aws securityhub decline-invitations --account-ids "123456789012"
```

Aufheben der Zuordnung von Mitgliedskonten in Security Hub CSPM

Note

Wir empfehlen, AWS Organizations anstelle von Security Hub CSPM-Einladungen zu verwenden, um Ihre Mitgliedskonten zu verwalten. Weitere Informationen finden Sie unter [Security Hub CSPM für mehrere Konten verwalten mit AWS Organizations](#).

Ein AWS Security Hub Cloud Security Posture Management (CSPM) -Administratorkonto kann die Zuordnung zu einem Mitgliedskonto aufheben, sodass keine Ergebnisse mehr von diesem Konto empfangen und angezeigt werden. Sie müssen die Zuordnung zu einem Mitgliedskonto aufheben, bevor Sie es löschen können.

Wenn Sie die Zuordnung zu einem Mitgliedskonto aufheben, verbleibt es in Ihrer Liste der Mitgliedskonten mit dem Status Entfernt (Getrennt). Ihr Konto wird aus den Administratorkontoinformationen für das Mitgliedskonto entfernt.

Um weiterhin Ergebnisse für das Konto zu erhalten, können Sie die Einladung erneut versenden. Um das Mitgliedskonto vollständig zu entfernen, können Sie das Mitgliedskonto löschen.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um ein manuell eingeladenes Mitgliedskonto vom Administratorkonto zu trennen.

Security Hub CSPM console

So trennen Sie die Zuordnung eines manuell eingeladenen Mitgliedskontos

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>

Melden Sie sich mit den Anmeldeinformationen des Administratorkontos an.

2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Konfiguration aus.
3. Wählen Sie im Abschnitt Konten die Konten aus, deren Verknüpfung Sie aufheben möchten.
4. Wählen Sie „Aktionen“ und anschließend „Konto trennen“.

Security Hub CSPM API

Um die Verbindung zu einem manuell eingeladenen Mitgliedskonto zu trennen

Rufen Sie die [DisassociateMembers](#)API vom Administratorkonto aus auf. Sie müssen die AWS-Konto IDs Mitgliedskonten angeben, deren Verknüpfung Sie aufheben möchten. Verwenden Sie den [ListMembers](#)Vorgang, um eine Liste der Mitgliedskonten anzuzeigen.

AWS CLI

Um die Zuordnung zu einem manuell eingeladenen Mitgliedskonto aufzuheben

Führen Sie den [disassociate-members](#) Befehl vom Administratorkonto aus. Sie müssen die AWS-Konto IDs Mitgliedskonten angeben, deren Verknüpfung Sie aufheben möchten. Führen Sie den [list-members](#) Befehl aus, um eine Liste der Mitgliedskonten anzuzeigen.

```
aws securityhub disassociate-members --account-ids <accountIds>
```

Beispiel

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

Löschen von Mitgliedskonten in Security Hub CSPM

Note

Wir empfehlen, AWS Organizations anstelle von Security Hub CSPM-Einladungen zu verwenden, um Ihre Mitgliedskonten zu verwalten. Weitere Informationen finden Sie unter [Security Hub CSPM für mehrere Konten verwalten mit AWS Organizations](#).

Als Administratorkonto für AWS Security Hub Cloud Security Posture Management (CSPM) können Sie Mitgliedskonten löschen, die auf Einladung hinzugefügt wurden. Bevor Sie ein aktiviertes Konto löschen können, müssen Sie die Zuordnung aufheben.

Wenn Sie ein Mitgliedskonto löschen, wird es vollständig aus der Liste entfernt. Um die Mitgliedschaft des Kontos wiederherzustellen, müssen Sie es hinzufügen und erneut einladen, als ob es sich um ein völlig neues Mitgliedskonto handeln würde.

Sie können keine Konten löschen, die zu einer Organisation gehören und die mithilfe der Integration mit verwaltet werden AWS Organizations.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten zum Löschen manuell eingeladener Mitgliedskonten.

Security Hub CSPM console

Um ein manuell eingeladenes Mitgliedskonto zu löschen

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>

Melden Sie sich mit dem Administratorkonto an.

2. Wählen Sie im Navigationsbereich Einstellungen und dann Konfiguration aus.
3. Wählen Sie den Tab Einladungskonten aus. Wählen Sie dann die Konten aus, die Sie löschen möchten.
4. Wählen Sie Aktionen und anschließend Löschen aus. Diese Option ist nur verfügbar, wenn Sie die Kontoverknüpfung aufgehoben haben. Sie müssen die Zuordnung zu einem Mitgliedskonto aufheben, bevor es gelöscht werden kann.

Security Hub CSPM API

Um ein manuell eingeladenes Mitgliedskonto zu löschen

Rufen Sie die [DeleteMembers](#)API vom Administratorkonto aus auf. Sie müssen die AWS-Konto IDs Mitgliedskonten angeben, die Sie löschen möchten. Rufen Sie die [ListMembers](#)API auf, um die Liste der Mitgliedskonten abzurufen.

AWS CLI

Um ein manuell eingeladenes Mitgliedskonto zu löschen

Führen Sie den [delete-members](#)Befehl vom Administratorkonto aus. Sie müssen die AWS-Konto IDs Mitgliedskonten angeben, die Sie löschen möchten. Führen Sie den [list-members](#)Befehl aus, um die Liste der Mitgliedskonten abzurufen.

```
aws securityhub delete-members --account-ids <memberAccountIDs>
```

Beispiel

```
aws securityhub delete-members --account-ids "123456789111" "123456789222"
```

Trennung von einem Security Hub CSPM-Administratorkonto

Note

Wir empfehlen, AWS Organizations anstelle von Security Hub CSPM-Einladungen zu verwenden, um Ihre Mitgliedskonten zu verwalten. Weitere Informationen finden Sie unter [Security Hub CSPM für mehrere Konten verwalten mit AWS Organizations](#).

Wenn Ihr Konto auf Einladung als AWS Security Hub Cloud Security Posture Management (CSPM) -Mitgliedskonto hinzugefügt wurde, können Sie das Mitgliedskonto vom Administratorkonto trennen. Nachdem Sie die Zuordnung zu einem Mitgliedskonto aufgehoben haben, sendet Security Hub CSPM keine Ergebnisse aus dem Konto an das Administratorkonto.

Mitgliedskonten, die mithilfe der Integration mit verwaltet werden, AWS Organizations können ihre Konten nicht vom Administratorkonto trennen. Nur der delegierte Security Hub CSPM-Administrator kann die Zuordnung von Mitgliedskonten aufheben, die mit Organizations verwaltet werden.

Wenn Sie die Verbindung zu Ihrem Administratorkonto trennen, verbleibt Ihr Konto in der Mitgliederliste des Administratorkontos mit dem Status Kündigt. Das Administratorkonto erhält jedoch keine Ergebnisse für Ihr Konto.

Nachdem Sie sich vom Administratorkonto getrennt haben, bleibt die Einladung, Mitglied zu werden, weiterhin bestehen. Sie können die Einladung in future erneut annehmen.

Security Hub CSPM console

Um die Verbindung zu Ihrem Administratorkonto zu trennen

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Einstellungen und dann Konten aus.
3. Deaktivieren Sie im Abschnitt Administratorkonto die Option Annehmen und wählen Sie dann Aktualisieren aus.

Security Hub CSPM API

Um die Verbindung zu Ihrem Administratorkonto zu trennen

Rufen Sie die API auf [DisassociateFromAdministratorAccount](#).

AWS CLI

Um die Verbindung zu Ihrem Administratorkonto zu trennen

Führen Sie den Befehl [disassociate-from-administrator-account](#) aus.

```
aws securityhub disassociate-from-administrator-account
```

 Note

Die Security Hub CSPM-Konsole wird weiterhin verwendet.

`DisassociateFromMasterAccount` Sie wird irgendwann auf Verwendung umgestellt. `DisassociateFromAdministratorAccount` Alle IAM-Richtlinien, die speziell den Zugriff auf diese Funktion regeln, müssen weiterhin verwendet `DisassociateFromMasterAccount` werden. Sie sollten Ihre Richtlinien auch ergänzen `DisassociateFromAdministratorAccount`, um sicherzustellen, dass nach Beginn der Nutzung `DisassociateFromAdministratorAccount` der Konsole die richtigen Berechtigungen vorhanden sind.

Umstellung auf Organizations zur Verwaltung von Konten in Security Hub CSPM

Wenn Sie Konten manuell in AWS Security Hub Cloud Security Posture Management (CSPM) verwalten, müssen Sie potenzielle Mitgliedskonten einladen und jedes Mitgliedskonto in jedem Konto separat konfigurieren. AWS-Region

Durch die Integration von Security Hub CSPM und AWS Organizations können Sie das Senden von Einladungen überflüssig machen und mehr Kontrolle darüber gewinnen, wie Security Hub CSPM in Ihrem Unternehmen konfiguriert und angepasst wird. Aus diesem Grund empfehlen wir, AWS Organizations anstelle von Security Hub CSPM-Einladungen zur Verwaltung Ihrer Mitgliedskonten zu verwenden. Weitere Informationen finden Sie unter [Security Hub CSPM für mehrere Konten verwalten mit AWS Organizations](#).

Es ist möglich, einen kombinierten Ansatz zu verwenden, bei dem Sie die AWS Organizations Integration verwenden, aber auch Konten außerhalb Ihrer Organisation manuell einladen. Wir empfehlen jedoch, ausschließlich die Organizations-Integration zu verwenden. Die [zentrale Konfiguration](#), eine Funktion, mit der Sie Security Hub CSPM über mehrere Konten und Regionen hinweg verwalten können, ist nur bei der Integration mit Organizations verfügbar.

In diesem Abschnitt wird beschrieben, wie Sie von der manuellen Kontoverwaltung auf Einladungsbasis zur Verwaltung von Konten mit übergehen können. AWS Organizations

Integration von Security Hub CSPM mit AWS Organizations

Zunächst müssen Sie Security Hub CSPM und integrieren. AWS Organizations

Sie können diese Dienste integrieren, indem Sie die folgenden Schritte ausführen:

- Erstellen Sie eine Organisation in AWS Organizations. Anweisungen finden Sie im AWS Organizations Benutzerhandbuch unter [Organisation erstellen](#).
- Geben Sie im Verwaltungskonto Organizations ein delegiertes Security Hub-CSPM-Administratorkonto an.

 Note

Das Organisationsverwaltungskonto kann nicht als DA-Konto festgelegt werden.

Detaillierte Anweisungen finden Sie unter [Integration von Security Hub CSPM mit AWS Organizations](#).

Indem Sie die vorherigen Schritte ausführen, gewähren Sie [vertrauenswürdigen Zugriff](#) für Security Hub CSPM in. AWS Organizations Dadurch wird auch Security Hub CSPM in der aktuellen Version AWS-Region für das delegierte Administratorkonto aktiviert.

Der delegierte Administrator kann die Organisation in Security Hub CSPM verwalten, indem er in erster Linie die Konten der Organisation als Security Hub CSPM-Mitgliedskonten hinzufügt. Der Administrator kann auch auf bestimmte Security Hub CSPM-Einstellungen, Daten und Ressourcen für diese Konten zugreifen.

Wenn Sie zur Kontoverwaltung mit Organizations wechseln, werden Konten, die auf Einladung basieren, nicht automatisch zu Security Hub CSPM-Mitgliedern. Nur die Konten, die Sie zu Ihrer neuen Organisation hinzufügen, können Security Hub CSPM-Mitglieder werden.

Nach der Aktivierung der Integration können Sie Konten bei Organizations verwalten. Weitere Informationen finden Sie unter [Security Hub CSPM für mehrere Konten verwalten mit AWS Organizations](#). Die Kontoverwaltung variiert je nach Konfigurationstyp Ihrer Organisation.

Zulässige Aktionen von Administrator- und Mitgliedskonten in Security Hub CSPM

Administrator- und Mitgliedskonten haben Zugriff auf die in den folgenden Tabellen aufgeführten AWS Security Hub Cloud Security Posture Management (CSPM) -Aktionen. In den Tabellen haben die Werte die folgende Bedeutung:

- **Beliebig** — Das Konto kann die Aktion für jedes Mitgliedskonto unter demselben Administrator ausführen.
- **Aktuell** — Das Konto kann die Aktion nur für sich selbst ausführen (das Konto, bei dem Sie derzeit angemeldet sind).
- **Dash** — Zeigt an, dass das Konto die Aktion nicht ausführen kann.

Wie in den Tabellen angegeben, hängen die zulässigen Aktionen davon ab, ob Sie eine Integration vornehmen AWS Organizations und welchen Konfigurationstyp Ihre Organisation verwendet. Informationen zum Unterschied zwischen zentraler und lokaler Konfiguration finden Sie unter [Konten verwalten mit AWS Organizations](#).

Security Hub CSPM kopiert die Ergebnisse des Mitgliedskontos nicht in das Administratorkonto. In Security Hub CSPM werden alle Ergebnisse für ein bestimmtes Konto in einer bestimmten Region erfasst. In jeder Region kann das Administratorkonto die Ergebnisse für seine Mitgliedskonten in dieser Region einsehen und verwalten.

Wenn Sie eine Aggregationsregion festlegen, kann das Administratorkonto die Ergebnisse von Mitgliedskonten aus verknüpften Regionen anzeigen und verwalten, die in die Aggregationsregion repliziert werden. [Weitere Informationen zur regionsübergreifenden Aggregation finden Sie unter Regionsübergreifende Aggregation](#).

In den folgenden Tabellen werden die Standardberechtigungen für Administrator- und Mitgliedskonten angegeben. Sie können benutzerdefinierte IAM-Richtlinien verwenden, um den Zugriff auf die Features und Funktionen von Security Hub CSPM weiter einzuschränken. Anleitungen und Beispiele finden Sie im Blogbeitrag [Aligning IAM-Policies to User Personas for AWS Security Hub Cloud Security Posture Management \(CSPM\)](#).

Zulässige Aktionen, wenn Sie in Organizations integrieren und die zentrale Konfiguration verwenden

Administrator- und Mitgliedskonten können wie folgt auf Security Hub CSPM-Aktionen zugreifen, wenn Sie eine Integration mit Organizations durchführen und die zentrale Konfiguration verwenden.

Aktion	Delegiertes Security Hub-CSPM-Administratorkonto	Zentral verwaltetes Mitgliedskonto	Selbstverwaltetes Mitgliedskonto
Security Hub CSPM-Konfigurationsrichtlinien erstellen und verwalten	Für selbst und zentral verwaltete Konten	–	–
Organisationskonten anzeigen	Any	–	–
Mitgliedskonto trennen	Any	–	–
Mitgliedskonto löschen	Jedes Konto, das nicht zur Organisation gehört	–	–
Security Hub CSPM deaktivieren	Für Girokonten und zentral verwaltete Konten	–	Aktuell (muss vom Administratorkonto getrennt werden)
Ergebnisse und Fundverlauf anzeigen	Any	Aktuell	Aktuell
Ergebnisse aktualisieren	Any	Aktuell	Aktuell
Insight-Ergebnisse anzeigen	Any	Aktuell	Aktuell
Kontrolldetails anzeigen	Any	Aktuell	Aktuell
Schalten Sie konsolidierte Kontrolle ergebnisse ein oder aus	Any	–	–

Aktion	Delegiertes Security Hub-CSPM-Administratorkonto	Zentral verwaltetes Mitgliedskonto	Selbstverwaltetes Mitgliedskonto
Aktivieren und deaktivieren Sie Standards	Für Girokonten und zentral verwaltete Konten	–	Aktuell
Steuerungen aktivieren und deaktivieren	Für Girokonten und zentral verwaltete Konten	–	Aktuell
Integrationen aktivieren und deaktivieren	Aktuell	Aktuell	Aktuell
Konfigurieren Sie die regionsübergreifende Aggregation	Any	–	–
Wählen Sie die Heimatregion und die verknüpften Regionen	Beliebig (Sie müssen die zentrale Konfiguration beenden und neu starten, um die Heimatregion zu ändern)	–	–
Konfigurieren Sie benutzerdefinierte Aktionen	Aktuell	Aktuell	Aktuell
Konfigurieren Sie Automatisierungsregeln	Any	–	–
Konfigurieren Sie benutzerdefinierte Einblicke	Aktuell	Aktuell	Aktuell

Zulässige Aktionen, wenn Sie eine Integration mit Organizations durchführen und die lokale Konfiguration verwenden

Administrator- und Mitgliedskonten können wie folgt auf Security Hub CSPM-Aktionen zugreifen, wenn Sie eine Integration mit Organizations durchführen und die lokale Konfiguration verwenden.

Aktion	Delegiertes Security Hub-CSPM-Administratorkonto	Mitgliedskonto
Security Hub CSPM-Konfigurationsrichtlinien erstellen und verwalten	–	–
Organisationskonten anzeigen	Any	–
Mitgliedskonto trennen	Any	–
Mitgliedskonto löschen	–	–
Security Hub CSPM deaktivieren	–	Aktuell (wenn das Konto vom delegierten Administrator getrennt ist)
Ergebnisse und Fundverlauf anzeigen	Any	Aktuell
Ergebnisse aktualisieren	Any	Aktuell
Insight-Ergebnisse anzeigen	Any	Aktuell
Kontrolldetails anzeigen	Any	Aktuell
Schalten Sie konsolidierte Kontrollergebnisse ein oder aus	Any	–
Aktivieren und deaktivieren Sie Standards	Aktuell	Aktuell

Aktion	Delegiertes Security Hub-CSPM-Administratorkonto	Mitgliedskonto
Automatisches Aktivieren von Security Hub CSPM und Standardstandards in neuen Unternehmenskonten	Für Girokonten und neue Organisationskonten	–
Steuerelemente aktivieren und deaktivieren	Aktuell	Aktuell
Aktiviere und deaktiviere Integrationen	Aktuell	Aktuell
Konfigurieren Sie die regionsübergreifende Aggregation	Any	–
Konfigurieren Sie benutzerdefinierte Aktionen	Aktuell	Aktuell
Konfigurieren Sie Automatisierungsregeln	Any	–
Konfigurieren Sie benutzerdefinierte Einblicke	Aktuell	Aktuell

Zulässige Aktionen für Konten, die auf Einladungen basieren

Administrator- und Mitgliedskonten können wie folgt auf Security Hub CSPM-Aktionen zugreifen, wenn Sie die einladungsbasierte Methode verwenden, um Konten manuell zu verwalten, anstatt sie zu integrieren. AWS Organizations

Aktion	Security Hub CSPM-Administratorkonto	Mitgliedskonto
Security Hub CSPM-Konfigurationsrichtlinien erstellen und verwalten	–	–
Organisationskonten anzeigen	Any	–
Mitgliedskonto trennen	Any	Aktuell
Mitgliedskonto löschen	Any	–
Security Hub CSPM deaktivieren	Aktuell (wenn keine aktivierten Mitgliedskonten vorhanden sind)	Aktuell (wenn das Konto vom Administratorkonto getrennt ist)
Ergebnisse und Fundverlauf anzeigen	Any	Aktuell
Ergebnisse aktualisieren	Any	Aktuell
Insight-Ergebnisse anzeigen	Any	Aktuell
Kontrolldetails anzeigen	Any	Aktuell
Schalten Sie konsolidierte Kontrollergebnisse ein oder aus	Any	–
Aktivieren und deaktivieren Sie Standards	Aktuell	Aktuell
Automatisches Aktivieren von Security Hub CSPM und Standardstandards in neuen Unternehmenskonten	–	–

Aktion	Security Hub CSPM-Administratorkonto	Mitgliedskonto
Steuerungen aktivieren und deaktivieren	Aktuell	Aktuell
Aktiviere und deaktiviere Integrationen	Aktuell	Aktuell
Konfigurieren Sie die regionsübergreifende Aggregation	Any	–
Konfigurieren Sie benutzerdefinierte Aktionen	Aktuell	Aktuell
Konfigurieren Sie Automatisierungsregeln	Any	–
Konfigurieren Sie benutzerdefinierte Einblicke	Aktuell	Aktuell

Auswirkung von Kontoaktionen auf Security Hub CSPM-Daten

Diese Kontoaktionen haben die folgenden Auswirkungen auf die AWS Security Hub Cloud Security Posture Management (CSPM) -Daten.

Security Hub CSPM ist deaktiviert

Wenn Sie die [zentrale Konfiguration](#) verwenden, kann der delegierte Administrator (DA) Security Hub CSPM-Konfigurationsrichtlinien erstellen, die AWS Security Hub Cloud Security Posture Management (CSPM) in bestimmten Konten und Organisationseinheiten deaktivieren (). OUs In diesem Fall ist Security Hub CSPM in den angegebenen Konten sowie OUs in Ihrer Heimatregion und allen verknüpften Regionen deaktiviert. Wenn Sie die zentrale Konfiguration nicht verwenden, müssen Sie Security Hub CSPM in jedem Konto und jeder Region, in der Sie es aktiviert haben, separat deaktivieren. Sie können die zentrale Konfiguration nicht verwenden, wenn Security Hub CSPM im DA-Konto deaktiviert ist.

Für das Administratorkonto werden keine Ergebnisse generiert oder aktualisiert, wenn Security Hub CSPM im Administratorkonto deaktiviert ist. Bestehende archivierte Ergebnisse werden nach 30 Tagen gelöscht. Bestehende aktive Ergebnisse werden nach 90 Tagen gelöscht.

Integrationen mit anderen AWS-Services werden entfernt.

Aktiviert Sicherheitsstandards und Kontrollen sind deaktiviert.

Andere Security Hub CSPM-Daten und -Einstellungen, einschließlich benutzerdefinierter Aktionen, Einblicke und Abonnements für Produkte von Drittanbietern, werden 90 Tage lang aufbewahrt.

Das Mitgliedskonto wurde vom Administratorkonto getrennt

Wenn die Verknüpfung eines Mitgliedskontos mit dem Administratorkonto getrennt wird, verliert das Administratorkonto die Berechtigung, Ergebnisse im Mitgliedskonto einzusehen. Security Hub CSPM ist jedoch weiterhin in beiden Konten aktiviert.

Wenn Sie die zentrale Konfiguration verwenden, kann der DA Security Hub CSPM nicht für ein Mitgliedskonto konfigurieren, das vom DA-Konto getrennt ist.

Benutzerdefinierte Einstellungen oder Integrationen, die für das Administratorkonto definiert sind, werden nicht auf Ergebnisse aus dem früheren Mitgliedskonto angewendet. Wenn die Konten beispielsweise getrennt wurden, haben Sie möglicherweise eine benutzerdefinierte Aktion im Administratorkonto, die als Ereignismuster in einer EventBridge Amazon-Regel verwendet wird. Diese benutzerdefinierte Aktion kann jedoch nicht im Mitgliedskonto verwendet werden.

In der Kontenliste für das Security Hub CSPM-Administratorkonto hat ein entferntes Konto den Status Getrennt.

Das Mitgliedskonto wurde aus einer Organisation entfernt

Wenn ein Mitgliedskonto aus einer Organisation entfernt wird, verliert das Security Hub CSPM-Administratorkonto die Berechtigung, Ergebnisse im Mitgliedskonto einzusehen. Security Hub CSPM ist jedoch weiterhin in beiden Konten mit denselben Einstellungen aktiviert, die sie vor dem Entfernen hatten.

Wenn Sie die zentrale Konfiguration verwenden, können Sie Security Hub CSPM nicht für ein Mitgliedskonto konfigurieren, nachdem es aus der Organisation entfernt wurde, zu der der delegierte Administrator gehört. Das Konto behält jedoch die Einstellungen bei, die es vor der Entfernung hatte, sofern Sie sie nicht manuell ändern.

In der Kontenliste für das Security Hub CSPM-Administratorkonto hat ein entferntes Konto den Status **Gelöscht**.

Das Konto ist gesperrt

Wenn ein gesperrt AWS-Konto wird, verliert das Konto die Erlaubnis, seine Ergebnisse in Security Hub CSPM einzusehen. Für dieses Konto werden keine Ergebnisse generiert oder aktualisiert. Das Administratorkonto für ein gesperrtes Konto kann die vorhandenen Ergebnisse für das Konto einsehen.

Bei einem Unternehmenskonto kann sich der Status des Mitgliedskontos auch in Konto gesperrt ändern. Dies ist der Fall, wenn das Konto gleichzeitig gesperrt wird, während das Administratorkonto versucht, das Konto zu aktivieren. Das Administratorkonto für ein gesperrtes Konto kann die Ergebnisse für dieses Konto nicht einsehen. Andernfalls hat der Status „Gesperrt“ keinen Einfluss auf den Status des Mitgliedskontos.

Wenn Sie die zentrale Konfiguration verwenden, schlägt die Richtlinienzuweisung fehl, wenn der delegierte Administrator versucht, einem gesperrten Konto eine Konfigurationsrichtlinie zuzuordnen.

Nach 90 Tagen wird das Konto entweder gekündigt oder reaktiviert. Wenn das Konto reaktiviert wird, werden seine Security Hub CSPM-Berechtigungen wiederhergestellt. Wenn das Mitgliedskonto den Status **Konto gesperrt** hat, muss das Administratorkonto das Konto manuell aktivieren.

Das Konto ist geschlossen

Wenn ein geschlossen AWS-Konto wird, reagiert Security Hub CSPM wie folgt auf das Schließen.

Wenn es sich bei dem Konto um ein Security Hub CSPM-Administratorkonto handelt, wird es als Administratorkonto entfernt und alle Mitgliedskonten werden entfernt. Wenn es sich bei dem Konto um ein Mitgliedskonto handelt, wird es getrennt und als Mitglied aus dem Security Hub CSPM-Administratorkonto entfernt.

Security Hub CSPM bewahrt bestehende archivierte Ergebnisse 30 Tage lang im Konto auf. Bei einem Kontrollbefund basiert die Berechnung von 30 Tagen auf dem Wert für das `UpdatedAt` Feld, in dem das Ergebnis festgestellt wurde. Bei einem anderen Befundtyp basiert die Berechnung auf dem Wert für das `ProcessedAt` Feld `UpdatedAt` oder des Ergebnisses, je nachdem, welches Datum das späteste ist. Nach Ablauf dieser 30-tägigen Frist löscht Security Hub CSPM den Befund dauerhaft aus dem Konto.

Security Hub CSPM speichert bestehende aktive Ergebnisse 90 Tage lang im Konto. Bei einem Kontrollbefund basiert die Berechnung von 90 Tagen auf dem Wert für das UpdatedAt Feld, in dem das Ergebnis festgestellt wurde. Bei einem anderen Befundtyp basiert die Berechnung auf dem Wert für das ProcessedAt Feld UpdatedAt oder des Ergebnisses, je nachdem, welches Datum das späteste ist. Am Ende dieses 90-Tage-Zeitraums löscht Security Hub CSPM den Befund dauerhaft aus dem Konto.

Zur längerfristigen Aufbewahrung vorhandener Ergebnisse können Sie die Ergebnisse in einen S3-Bucket exportieren. Sie können dies tun, indem Sie eine benutzerdefinierte Aktion mit einer EventBridge Amazon-Regel verwenden. Weitere Informationen finden Sie unter [Verwendung EventBridge für automatisierte Reaktionen und Problembehebungen](#).

 Important

Für Kunden, die sich angemeldet haben AWS GovCloud (US) Regions, erstellen Sie eine Sicherungskopie und löschen Sie dann Ihre Versicherungsdaten und andere Kontoressourcen, bevor Sie Ihr Konto schließen. Nachdem Sie Ihr Konto geschlossen haben, haben Sie keinen Zugriff mehr auf die Ressourcen und Daten.

Weitere Informationen finden Sie unter [Schließen](#) und AWS-Konto im AWS -Kontenverwaltung Referenzhandbuch.

Grundlegendes zur regionsübergreifenden Aggregation in Security Hub CSPM

Note

Die Aggregationsregion wird jetzt als Heimatregion bezeichnet. Einige Security Hub CSPM-API-Operationen verwenden immer noch den älteren Begriff Aggregationsregion.

Durch die Verwendung der regionsübergreifenden Aggregation in AWS Security Hub Cloud Security Posture Management (CSPM) können Sie Ergebnisse zusammenfassen, Updates und Erkenntnisse finden, den Compliance-Status und Sicherheitsbewertungen von mehreren AWS-Regionen zu einer einzigen Heimatregion kontrollieren. Anschließend können Sie all diese Daten von der Heimatregion aus verwalten.

Angenommen, Sie legen USA Ost (Nord-Virginia) als Heimatregion und USA West (Oregon) und USA West (Nordkalifornien) als verknüpfte Regionen fest. Wenn Sie die Ergebnisseite in USA Ost (Nord-Virginia) aufrufen, sehen Sie die Ergebnisse aus allen drei Regionen. Aktualisierungen dieser Ergebnisse spiegeln sich auch in allen drei Regionen wider.

Note

In AWS GovCloud (US) wird die regionsübergreifende Aggregation nur für Ergebnisse, Aktualisierungen und Erkenntnisse in allen Regionen unterstützt. AWS GovCloud (US) Insbesondere können Sie nur Ergebnisse, Aktualisierungen und Erkenntnisse zwischen AWS GovCloud (USA-Ost) und AWS GovCloud (US-West) zusammenfassen. In den Regionen China wird die regionsübergreifende Aggregation nur für Ergebnisse, Aktualisierungen und Erkenntnisse in den Regionen China unterstützt. Insbesondere können Sie nur Ergebnisse, Aktualisierungen und Erkenntnisse zwischen China (Peking) und China (Ningxia) zusammenfassen.

Wenn ein Steuerelement in einer verknüpften Region aktiviert, aber in der Heimatregion deaktiviert ist, können Sie den Konformitätsstatus des Steuerelements in der Heimatregion anzeigen, aber Sie können dieses Steuerelement nicht von der Heimatregion aus aktivieren oder deaktivieren. Die Ausnahme ist, wenn Sie die [zentrale Konfiguration](#) verwenden. Wenn Sie die zentrale Konfiguration

verwenden, kann der delegierte Security Hub CSPM-Administrator Steuerungen in der Heimatregion und verknüpften Regionen von der Heimatregion aus konfigurieren.

Wenn Sie eine Heimatregion festgelegt haben, berücksichtigen die [Sicherheitswerte](#) den Kontrollstatus in allen verknüpften Regionen. Um regionsübergreifende Sicherheitsbewertungen und Compliance-Status anzuzeigen, fügen Sie Ihrer IAM-Rolle, die Security Hub CSPM verwendet, die folgenden Berechtigungen hinzu:

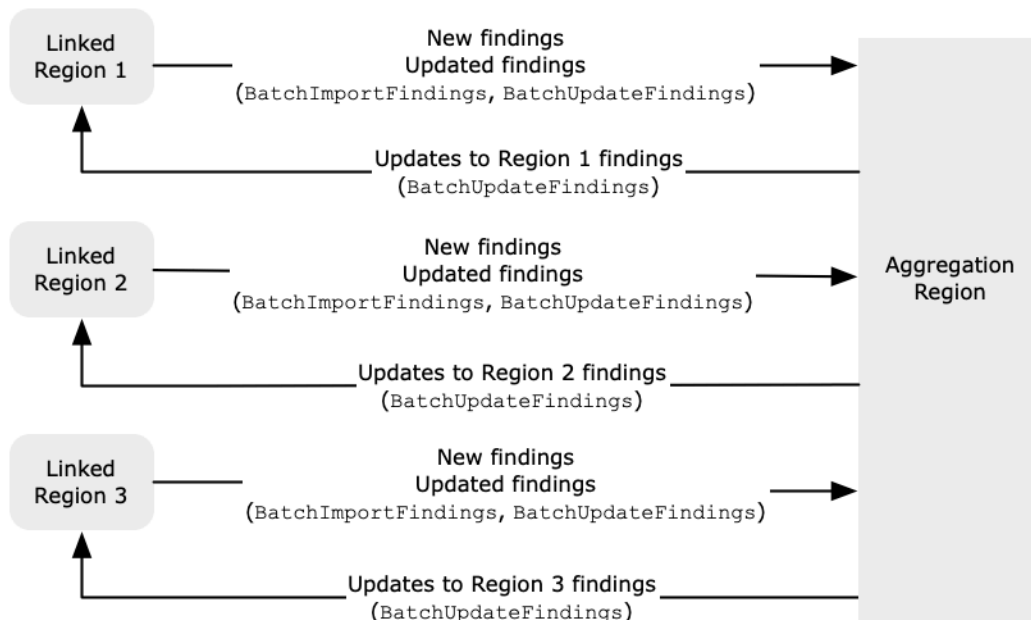
- [ListSecurityControlDefinitions](#)
- [BatchGetStandardsControlAssociations](#)
- [BatchUpdateStandardsControlAssociations](#)

Arten von Daten, die aggregiert sind

Wenn die regionsübergreifende Aggregation mit einer oder mehreren verknüpften Regionen aktiviert ist, repliziert Security Hub CSPM die folgenden Daten aus den verknüpften Regionen in die Heimatregion. Dies geschieht in jedem Konto, für das die regionsübergreifende Aggregation aktiviert ist.

- Funde
- Insights
- Kontrollieren Sie den Compliance-Status
- Sicherheitswerte

Zusätzlich zu den neuen Daten in der vorherigen Liste repliziert Security Hub CSPM auch Aktualisierungen dieser Daten zwischen den verknüpften Regionen und der Heimatregion. Updates, die in einer verknüpften Region vorgenommen werden, werden in die Heimatregion repliziert. Aktualisierungen, die in der Heimatregion vorgenommen werden, werden zurück in die verknüpfte Region repliziert. Wenn es in der Heimatregion und der verknüpften Region widersprüchliche Aktualisierungen gibt, wird das neueste Update verwendet.



Die regionsübergreifende Aggregation erhöht nicht die Kosten von Security Hub CSPM. Es fallen keine Gebühren an, wenn Security Hub CSPM neue Daten oder Updates repliziert.

In der Heimatregion bietet die Übersichtsseite einen Überblick über Ihre aktiven Ergebnisse in den verknüpften Regionen. Weitere Informationen finden Sie unter [Eine regionsübergreifende Zusammenfassung der Ergebnisse nach Schweregrad anzeigen](#). In anderen Bereichen auf der Übersichtsseite, in denen Ergebnisse analysiert werden, werden ebenfalls Informationen aus allen verknüpften Regionen angezeigt.

Ihre Sicherheitswerte in der Heimatregion werden berechnet, indem die Anzahl der bestandenen Kontrollen mit der Anzahl der aktivierten Kontrollen in allen verknüpften Regionen verglichen wird. Wenn ein Steuerelement in mindestens einer verknüpften Region aktiviert ist, ist es außerdem auf den Detailseiten zu den Sicherheitsstandards der Heimatregion sichtbar. Der Konformitätsstatus der Kontrollen auf den Seiten mit den Standarddetails spiegelt die Ergebnisse der verknüpften Regionen wider. Wenn eine mit einer Kontrolle verknüpfte Sicherheitsüberprüfung in einer oder mehreren verknüpften Regionen fehlschlägt, wird der Konformitätsstatus dieser Kontrolle auf den Standarddetailseiten der Heimatregion als Fehlgeschlagen angezeigt. Die Anzahl der Sicherheitsüberprüfungen umfasst Ergebnisse aus allen verknüpften Regionen.

Security Hub CSPM aggregiert nur Daten aus Regionen, in denen Security Hub CSPM für ein Konto aktiviert ist. Security Hub CSPM wird nicht automatisch für ein Konto aktiviert, das auf der regionsübergreifenden Aggregationskonfiguration basiert.

Es ist möglich, die regionsübergreifende Aggregation zu aktivieren, ohne dass verknüpfte Regionen ausgewählt werden. In diesem Fall findet keine Datenreplikation statt.

Aggregation für Administrator- und Mitgliedskonten

Eigenständige Konten, Mitgliedskonten und Administratorkonten können die regionsübergreifende Aggregation konfigurieren. Falls von einem Administrator konfiguriert, ist das Vorhandensein des Administratorkontos unerlässlich, damit die regionsübergreifende Aggregation in verwalteten Konten funktioniert. Wenn das Administratorkonto entfernt oder von einem Mitgliedskonto getrennt wird, wird die regionsübergreifende Aggregation für das Mitgliedskonto beendet. Dies gilt auch dann, wenn für das Konto die regionsübergreifende Aggregation aktiviert war, bevor die Beziehung zwischen Administrator und Mitglied aufgenommen wurde.

Wenn ein Administratorkonto die regionsübergreifende Aggregation aktiviert, repliziert Security Hub CSPM die Daten, die das Administratorkonto in allen verknüpften Regionen generiert, in die Heimatregion. Darüber hinaus identifiziert Security Hub CSPM die Mitgliedskonten, die diesem Administrator zugeordnet sind, und jedes Mitgliedskonto erbt die regionsübergreifenden Aggregationseinstellungen des Administrators. Security Hub CSPM repliziert die Daten, die ein Mitgliedskonto in allen verknüpften Regionen generiert, in die Heimatregion.

Der Administrator kann von allen Mitgliedskonten in den verwalteten Regionen aus auf Sicherheitsergebnisse zugreifen und diese verwalten. Als Security Hub CSPM-Administrator müssen Sie jedoch in der Heimatregion angemeldet sein, um aggregierte Daten aus allen Mitgliedskonten und verknüpften Regionen einsehen zu können.

Als Security Hub CSPM-Mitgliedskonto müssen Sie in der Heimatregion angemeldet sein, um aggregierte Daten aus Ihrem Konto aus allen verknüpften Regionen einsehen zu können. Mitgliedskonten sind nicht berechtigt, Daten von anderen Mitgliedskonten einzusehen.

Ein Administratorkonto kann Mitgliedskonten manuell einladen oder als delegierter Administrator einer Organisation fungieren, in die integriert AWS Organizations ist. Bei einem [Mitgliedskonto mit manueller Einladung](#) muss der Administrator das Konto aus der Heimatregion und allen verknüpften Regionen einladen, damit die regionsübergreifende Aggregation funktioniert. Darüber hinaus muss für das Mitgliedskonto Security Hub CSPM in der Heimatregion und allen verknüpften Regionen aktiviert sein, damit der Administrator die Ergebnisse des Mitgliedskontos einsehen kann. Wenn Sie die Heimatregion nicht für andere Zwecke verwenden, können Sie die Security Hub CSPM-Standards und -Integrationen in dieser Region deaktivieren, um Gebühren zu vermeiden.

Wenn Sie die regionsübergreifende Aggregation verwenden möchten und über mehrere Administratorkonten verfügen, empfehlen wir Ihnen, die folgenden bewährten Methoden zu befolgen:

- Jedes Administratorkonto hat unterschiedliche Mitgliedskonten.
- Jedes Administratorkonto hat in allen Regionen dieselben Mitgliedskonten.
- Jedes Administratorkonto verwendet eine andere Heimatregion.

 Note

Informationen darüber, wie sich die regionsübergreifende Aggregation auf die zentrale Konfiguration auswirkt, finden Sie unter [Auswirkungen der zentralen Konfiguration auf die regionsübergreifende Aggregation](#)

Auswirkungen der zentralen Konfiguration auf die regionsübergreifende Aggregation

Die zentrale Konfiguration ist eine optionale Funktion in AWS Security Hub Cloud Security Posture Management (CSPM), die Sie verwenden können, wenn Sie sie integrieren. AWS Organizations Wenn Sie die zentrale Konfiguration verwenden, kann das delegierte Administratorkonto den Security Hub CSPM-Dienst, die Standards und Kontrollen für Konten und Organisationseinheiten (OU) in der Organisation konfigurieren. Um Konten und zu konfigurieren OUs, erstellt der delegierte Administrator Security Hub CSPM-Konfigurationsrichtlinien. Mithilfe von Konfigurationsrichtlinien kann definiert werden, ob Security Hub CSPM aktiviert oder deaktiviert ist und welche Standards und Kontrollen aktiviert sind. Der delegierte Administrator ordnet Konfigurationsrichtlinien bestimmten Konten oder dem Stammkonto (der gesamten Organisation) zu. OUs

Der delegierte Administrator kann Konfigurationsrichtlinien für die Organisation nur von der Heimatregion aus erstellen und verwalten. Darüber hinaus werden Konfigurationsrichtlinien in der Heimatregion und allen verknüpften Regionen wirksam. Sie können keine Konfigurationsrichtlinie erstellen, die nur in einigen verknüpften Regionen gilt und in anderen nicht. Informationen zur regionsübergreifenden Aggregation finden Sie unter [Regionsübergreifende Aggregation](#).

Um die zentrale Konfiguration verwenden zu können, müssen Sie eine Heimatregion angeben. Optional können Sie eine oder mehrere Regionen als verknüpfte Regionen auswählen. Sie können sich auch dafür entscheiden, eine Heimatregion ohne verknüpfte Regionen festzulegen.

Eine Änderung Ihrer regionsübergreifenden Aggregationseinstellungen kann sich auf Ihre Konfigurationsrichtlinien auswirken. Wenn Sie eine verknüpfte Region hinzufügen, werden Ihre Konfigurationsrichtlinien in dieser Region wirksam. Wenn es sich bei der Region um eine [Opt-in-Region](#) handelt, muss die Region aktiviert sein, damit Ihre Konfigurationsrichtlinien dort wirksam werden. Umgekehrt sind die Konfigurationsrichtlinien in dieser Region nicht mehr wirksam, wenn Sie eine verknüpfte Region entfernen. In dieser Region behalten die Konten die Einstellungen bei, die sie hatten, als die verknüpfte Region entfernt wurde. Sie können diese Einstellungen ändern, müssen dies jedoch für jedes Konto und jede Region separat tun.

Wenn Sie die Heimatregion entfernen oder ändern, werden Ihre Konfigurationsrichtlinien und Richtlinienverknüpfungen gelöscht. Sie können in keiner Region mehr die zentrale Konfiguration verwenden oder Konfigurationsrichtlinien erstellen. Konten behalten die Einstellungen bei, die sie hatten, bevor die Heimatregion geändert oder entfernt wurde. Sie können diese Einstellungen jederzeit ändern. Da Sie die zentrale Konfiguration jedoch nicht mehr verwenden, müssen die Einstellungen für jedes Konto und jede Region separat geändert werden. Sie können die zentrale Konfiguration verwenden und erneut Konfigurationsrichtlinien erstellen, wenn Sie eine neue Heimatregion angeben.

Weitere Informationen zur zentralen Konfiguration finden Sie unter [Grundlegendes zur zentralen Konfiguration in Security Hub CSPM](#).

Aktivierung der regionsübergreifenden Aggregation

Note

Die Aggregationsregion wird jetzt als Heimatregion bezeichnet. Einige Security Hub CSPM-API-Operationen verwenden immer noch den älteren Begriff Aggregationsregion.

Sie müssen die regionsübergreifende Aggregation von der Region aus aktivieren AWS-Region , die Sie als Heimatregion festlegen möchten.

Um die regionsübergreifende Aggregation zu aktivieren, erstellen Sie eine Security Hub-CSPM-Ressource, die als Finding-Aggregator bezeichnet wird. Die Suchaggregator-Ressource gibt Ihre Heimatregion und verknüpfte Regionen (falls vorhanden) an.

Sie können keine Region AWS-Region , die standardmäßig deaktiviert ist, als Heimatregion verwenden. Eine Liste der Regionen, die standardmäßig deaktiviert sind, finden Sie unter [Aktivieren einer Region](#) in der Allgemeine AWS-Referenz.

Wenn Sie die regionsübergreifende Aggregation aktivieren, können Sie bei Bedarf eine oder mehrere verknüpfte Regionen angeben. Sie können auch wählen, ob neue Regionen automatisch verknüpft werden sollen, wenn Security Hub CSPM sie zu unterstützen beginnt und Sie sich für sie entschieden haben.

Security Hub CSPM console

Um die regionsübergreifende Aggregation zu aktivieren

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>
2. Melden Sie sich mit dem AWS-Region Selektor bei der Region an, die Sie als Aggregationsregion verwenden möchten.
3. Wählen Sie im Security Hub CSPM-Navigationsmenü Einstellungen und dann Regionen aus.
4. Wählen Sie unter Suchaggregation die Option Suchaggregation konfigurieren aus.

Standardmäßig ist die Heimatregion auf Keine Aggregationsregion gesetzt.

5. Wählen Sie unter Aggregationsregion die Option aus, um die aktuelle Region als Heimatregion festzulegen.
6. Wählen Sie optional für Verknüpfte Regionen die Regionen aus, aus denen Daten aggregiert werden sollen.
7. Um Daten aus neuen Regionen in der Partition automatisch zu aggregieren, sofern Security Hub CSPM sie unterstützt und Sie sich für sie entscheiden, wählen Sie future Regionen verknüpfen aus.
8. Wählen Sie Speichern.

Security Hub CSPM API

Verwenden Sie in der Region, die Sie als Heimatregion verwenden möchten, den [CreateFindingAggregator](#)Betrieb der Security Hub CSPM-API. Wenn Sie den verwenden AWS CLI, führen Sie den [create-finding-aggregator](#)Befehl aus.

Wählen Sie unter RegionLinkingMode eine der folgenden Optionen aus:

- ALL_REGIONS— Security Hub CSPM aggregiert Daten aus allen Regionen. Security Hub CSPM aggregiert auch Daten aus neuen Regionen, sobald diese unterstützt werden und Sie sich für sie entscheiden.

- **ALL_REGIONS_EXCEPT_SPECIFIED**— Security Hub CSPM aggregiert Daten aus allen Regionen mit Ausnahme der Regionen, die Sie ausschließen möchten. Security Hub CSPM aggregiert auch Daten aus neuen Regionen, sobald diese unterstützt werden und Sie sich für sie entscheiden. Wird verwendet `Regions`, um die Liste der Regionen bereitzustellen, die von der Aggregation ausgeschlossen werden sollen.
- **SPECIFIED_REGIONS**— Security Hub CSPM aggregiert Daten aus einer ausgewählten Liste von Regionen. Security Hub CSPM aggregiert Daten aus neuen Regionen nicht automatisch. Wird verwendet `Regions`, um die Liste der Regionen bereitzustellen, aus denen aggregiert werden soll.
- **NO_REGIONS**— Security Hub CSPM aggregiert keine Daten, da Sie keine verknüpften Regionen auswählen.

Im folgenden Beispiel wird die regionsübergreifende Aggregation konfiguriert. Die Heimatregion ist USA Ost (Nord-Virginia). Die verbundenen Regionen sind USA West (Nordkalifornien) und USA West (Oregon). Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub create-finding-aggregator --region us-east-1 --region-linking-mode SPECIFIED_REGIONS --regions us-west-1 us-west-2
```

Überprüfung der Einstellungen für die regionsübergreifende Aggregation

Note

Die Aggregationsregion wird jetzt als Heimatregion bezeichnet. Einige Security Hub CSPM-API-Operationen verwenden immer noch den älteren Begriff Aggregationsregion.

Sie können die aktuelle regionsübergreifende Aggregationskonfiguration in AWS Security Hub Cloud Security Posture Management (CSPM) von jedem aus anzeigen. AWS-Region Die Konfiguration umfasst die Heimatregion, die verknüpften Regionen (falls vorhanden) und ob neue Regionen automatisch verknüpft werden sollen, da Security Hub CSPM sie unterstützt.

Mitgliedskonten können die regionsübergreifenden Aggregationseinstellungen einsehen, die das Administratorkonto konfiguriert hat.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um Ihre aktuellen regionsübergreifenden Aggregationseinstellungen anzuzeigen.

Security Hub CSPM console

So zeigen Sie regionsübergreifende Aggregationseinstellungen an (Konsole)

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Einstellungen und dann die Registerkarte Regionen.

Wenn die regionsübergreifende Aggregation nicht aktiviert ist, wird auf der Registerkarte Regionen die Option zur Aktivierung der regionsübergreifenden Aggregation angezeigt. Nur Administratorkonten und eigenständige Konten können die regionsübergreifende Aggregation aktivieren.

Wenn die regionsübergreifende Aggregation aktiviert ist, werden auf der Registerkarte Regionen die folgenden Informationen angezeigt:

- Die Heimatregion
- Ob Ergebnisse, Erkenntnisse, Kontrollstatus und Sicherheitswerte aus neuen Regionen, die Security Hub CSPM unterstützt und für die Sie sich entscheiden, automatisch aggregiert werden sollen
- Die Liste der verknüpften Regionen (falls ausgewählt)

Security Hub CSPM API

So überprüfen Sie die Einstellungen für die regionsübergreifende Aggregation (Security Hub CSPM API)

Verwenden Sie den [GetFindingAggregator](#)Betrieb der Security Hub CSPM-API. Wenn Sie den verwenden AWS CLI, führen Sie den [get-finding-aggregator](#)Befehl aus.

Wenn Sie die Anfrage stellen, geben Sie den Suchaggregator-ARN an. Verwenden Sie die [ListFindingAggregators](#)Operation oder den [list-finding-aggregators](#)Befehl, um den Suchaggregator-ARN abzurufen.

Das folgende Beispiel zeigt die regionsübergreifenden Aggregationseinstellungen für den angegebenen Suchaggregator-ARN. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\), um die Lesbarkeit zu verbessern

```
$aws securityhub get-finding-aggregator --finding-aggregator-  
arn arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-  
e89b-12d3-a456-426652340000
```

Aktualisierung der regionsübergreifenden Aggregationseinstellungen

Note

Die Aggregationsregion wird jetzt als Heimatregion bezeichnet. Einige Security Hub CSPM-API-Operationen verwenden immer noch den älteren Begriff Aggregationsregion.

Sie können Ihre aktuellen regionsübergreifenden Aggregationseinstellungen in AWS Security Hub Cloud Security Posture Management (CSPM) aktualisieren, indem Sie die verknüpften Regionen oder die aktuelle Heimatregion ändern. Sie können auch ändern, ob Daten aus neuen Dateien, in AWS-Regionen denen Security Hub CSPM unterstützt wird, automatisch aggregiert werden sollen.

Änderungen an der regionsübergreifenden Aggregation werden für eine Opt-in-Region erst implementiert, wenn Sie die Region in Ihrer aktivieren. AWS-Konto Regionen, die am oder nach dem 20. März 2019 AWS eingeführt wurden, sind Opt-in-Regionen.

Wenn Sie die Aggregation von Daten aus einer verknüpften Region beenden, entfernt AWS Security Hub Cloud Security Posture Management (CSPM) keine vorhandenen aggregierten Daten aus dieser Region, auf die in der Heimatregion zugegriffen werden kann.

Sie können die Aktualisierungsverfahren in diesem Abschnitt nicht verwenden, um die Heimatregion zu ändern. Um die Heimatregion zu ändern, müssen Sie wie folgt vorgehen:

1. Beenden Sie die regionsübergreifende Aggregation. Detaillierte Anweisungen finden Sie unter [the section called “Die Aggregation wird beendet”](#).
2. Wechseln Sie zu der Region, die Sie als neue Heimatregion verwenden möchten.

3. Aktivieren Sie die regionsübergreifende Aggregation. Detaillierte Anweisungen finden Sie unter [the section called “Aggregation aktivieren”](#).

Sie müssen die regionsübergreifende Aggregationskonfiguration von der aktuellen Heimatregion aus aktualisieren.

Security Hub CSPM console

Um die verknüpften Regionen zu ändern

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>

Melden Sie sich bei der aktuellen Aggregationsregion an.

2. Wählen Sie im Security Hub CSPM-Navigationsmenü Einstellungen und dann Regionen aus.
3. Wählen Sie für Finding Aggregation die Option Bearbeiten aus.
4. Aktualisieren Sie für verknüpfte Regionen die ausgewählten verknüpften Regionen.
5. Ändern Sie bei Bedarf, ob die Option future Regionen verknüpfen ausgewählt ist. Diese Einstellung bestimmt, ob Security Hub CSPM neue Regionen automatisch verknüpft, wenn es Unterstützung für sie hinzufügt und Sie sich für sie entscheiden.
6. Wählen Sie Speichern.

Security Hub CSPM API

Verwenden Sie die Operation [UpdateFindingAggregator](#). Wenn Sie den verwenden AWS CLI, führen Sie den [update-finding-aggregator](#)Befehl aus. Um den Suchaggregator zu identifizieren, müssen Sie den Suchaggregator-ARN angeben. Verwenden Sie die [ListFindingAggregators](#)Operation oder den [list-finding-aggregators](#)Befehl, um den Suchaggregator-ARN abzurufen.

Wenn der Linkmodus ALL_REGIONS_EXCEPT_SPECIFIED oder istSPECIFIED_REGIONS, können Sie die Liste der ausgeschlossenen oder eingeschlossenen Regionen ändern. Wenn Sie den Modus für die Verknüpfung von Regionen auf ändern möchtenNO_REGIONS, sollten Sie keine Regionenliste angeben.

Wenn Sie die Liste der ausgeschlossenen oder eingeschlossenen Regionen ändern, müssen Sie die vollständige Liste zusammen mit den Aktualisierungen bereitstellen. Angenommen, Sie

aggregieren derzeit Ergebnisse aus USA Ost (Ohio) und möchten auch Ergebnisse aus USA West (Oregon) aggregieren. Sie müssen eine Regions Liste bereitstellen, die sowohl USA Ost (Ohio) als auch USA West (Oregon) enthält.

Im folgenden Beispiel wird die regionsübergreifende Aggregation für ausgewählte Regionen aktualisiert. Der Befehl wird von der aktuellen Heimatregion aus ausgeführt, die USA Ost (Nord-Virginia) ist. Die verknüpften Regionen sind USA West (Nordkalifornien) und USA West (Oregon). Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
aws securityhub update-finding-aggregator --region us-east-1 --finding-  
aggregator-arn arn:aws:securityhub:us-east-1:222222222222:finding-  
aggregator/123e4567-e89b-12d3-a456-426652340000 --region-linking-mode  
SPECIFIED_REGIONS --regions us-west-1 us-west-2
```

Die regionsübergreifende Aggregation wird beendet

Note

Die Aggregationsregion wird jetzt als Heimatregion bezeichnet. Einige Security Hub CSPM-API-Operationen verwenden immer noch den älteren Begriff Aggregationsregion.

Wenn Sie nicht möchten, dass AWS Security Hub Cloud Security Posture Management (CSPM) Daten aggregiert, können Sie Ihren Finding-Aggregator löschen. Alternativ können Sie Ihren Suchaggregator beibehalten, ihn aber nicht mit der Heimatregion verknüpfen AWS-Regionen, indem Sie den vorhandenen Aggregator auf den Verbindungsmodus aktualisieren. NO_REGIONS

Um Ihre Heimatregion zu ändern, müssen Sie Ihren aktuellen Suchaggregator löschen und einen neuen erstellen.

Wenn Sie Ihren Suchaggregator löschen, beendet Security Hub CSPM die Datenaggregation. Es entfernt keine vorhandenen aggregierten Daten aus der Heimatregion.

Der Suchaggregator (Konsole) wird gelöscht

Sie können Ihren Suchaggregator nur aus der aktuellen Heimatregion löschen.

In anderen Regionen als der Heimatregion wird im Bereich Finding Aggregation auf der Security Hub CSPM-Konsole eine Meldung angezeigt, dass Sie die Konfiguration in der Heimatregion bearbeiten müssen. Wählen Sie diese Nachricht, um einen Link anzuzeigen, über den Sie zur Heimatregion wechseln können.

Security Hub CSPM console

Um die regionsübergreifende Aggregation zu beenden (Konsole)

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>
2. Stellen Sie sicher, dass Sie in Ihrer aktuellen Heimatregion angemeldet sind.
3. Wählen Sie im Security Hub CSPM-Navigationsmenü Einstellungen und dann Regionen aus.
4. Wählen Sie unter Aggregation suchen die Option Bearbeiten aus.
5. Wählen Sie unter Aggregationsregion die Option Keine Aggregationsregion aus.
6. Wählen Sie Speichern.
7. Geben Sie im Bestätigungsdialogfeld in das Bestätigungsfeld Folgendes ein. **Confirm**
8. Wählen Sie Bestätigen aus.

Security Hub CSPM API

Verwenden Sie den [DeleteFindingAggregator](#)Betrieb der Security Hub CSPM-API. Wenn Sie den verwenden AWS CLI, führen Sie den [delete-finding-aggregator](#)Befehl aus.

Um den Suchaggregator zu identifizieren, der gelöscht werden soll, geben Sie den Suchaggregator-ARN an. Verwenden Sie die [ListFindingAggregators](#)Operation oder den [list-finding-aggregators](#)Befehl, um den Suchaggregator-ARN abzurufen.

Im folgenden Beispiel wird der Suchaggregator gelöscht. Der Befehl wird von der aktuellen Heimatregion aus ausgeführt, die USA Ost (Nord-Virginia) ist. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$aws securityhub delete-finding-aggregator arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-e89b-12d3-a456-426652340000 --region us-east-1
```

Grundlegendes zu den Sicherheitsstandards in Security Hub CSPM

In AWS Security Hub Cloud Security Posture Management (CSPM) besteht ein Sicherheitsstandard aus einer Reihe von Anforderungen, die auf regulatorischen Rahmenbedingungen, branchenüblichen Best Practices oder Unternehmensrichtlinien basieren. Einzelheiten zu den Standards, die Security Hub CSPM derzeit unterstützt, einschließlich der Sicherheitskontrollen, die für jeden Standard gelten, finden Sie unter [Standardreferenz für Security Hub CSPM](#)

Wenn Sie einen Standard aktivieren, aktiviert Security Hub CSPM automatisch alle Kontrollen, die für den Standard gelten. Security Hub CSPM führt dann Sicherheitsüberprüfungen an den Steuerelementen durch, wodurch Security Hub CSPM-Ergebnisse generiert werden. Sie können einzelne Steuerelemente bei Bedarf deaktivieren und später wieder aktivieren. Sie können einen Standard auch vollständig deaktivieren. Wenn Sie einen Standard deaktivieren, beendet Security Hub CSPM die Ausführung von Sicherheitsüberprüfungen für Kontrollen, die für den Standard gelten. Für die Kontrollen werden keine Ergebnisse mehr generiert.

Zusätzlich zu den Ergebnissen generiert Security Hub CSPM eine Sicherheitsbewertung für jeden Standard, den Sie aktivieren. Die Bewertung basiert auf dem Status der Kontrollen, die für den Standard gelten. Wenn Sie eine Aggregationsregion festlegen, spiegelt die Sicherheitsbewertung für einen Standard den Status der Kontrollen in allen verknüpften Regionen wider. Wenn Sie der Security Hub CSPM-Administrator einer Organisation sind, spiegelt die Bewertung den Status der Kontrollen für alle Konten in Ihrer Organisation wider. Weitere Informationen finden Sie unter [Berechnung von Sicherheitswerten](#).

Um Standards zu überprüfen und zu verwalten, können Sie die Security Hub CSPM-Konsole oder die Security Hub CSPM-API verwenden. Auf der Konsole werden auf der Seite Sicherheitsstandards alle Sicherheitsstandards angezeigt, die Security Hub CSPM derzeit unterstützt. Dies beinhaltet eine Beschreibung der einzelnen Standards und den aktuellen Status der Standards. Wenn Sie einen Standard aktivieren, können Sie auf dieser Seite auch auf zusätzliche Details zum Standard zugreifen. Sie können beispielsweise Folgendes überprüfen:

- Die aktuelle Sicherheitsbewertung für den Standard.
- Aggregierte Statistiken für Kontrollen, die für den Standard gelten.
- Eine Liste der Kontrollen, die für den Standard gelten und derzeit aktiviert sind, einschließlich des jeweiligen Konformitätsstatus.

- Eine Liste von Kontrollen, die für den Standard gelten, aber derzeit deaktiviert sind.

Für eine eingehendere Analyse können Sie die Daten filtern und sortieren und sich die Details der einzelnen Kontrollen ansehen, die für den Standard gelten.

Sie können Standards einzeln für ein einzelnes Konto aktivieren und AWS-Region. Um Zeit zu sparen und Konfigurationsabweichungen in Umgebungen mit mehreren Konten und mehreren Regionen zu reduzieren, empfehlen wir jedoch, die Standards über eine [zentrale Konfiguration](#) zu aktivieren und zu verwalten. Bei der zentralen Konfiguration kann der delegierte Security Hub CSPM-Administrator Richtlinien erstellen, die festlegen, wie ein Standard für mehrere Konten und Regionen konfiguriert werden soll.

Themen

- [Standardreferenz für Security Hub CSPM](#)
- [Einen Sicherheitsstandard aktivieren](#)
- [Überprüfung der Einzelheiten eines Sicherheitsstandards](#)
- [Durch das Ausschalten automatisch aktivierter Sicherheitsstandards](#)
- [Deaktivierung eines Sicherheitsstandards](#)

Standardreferenz für Security Hub CSPM

In AWS Security Hub Cloud Security Posture Management (CSPM) besteht ein Sicherheitsstandard aus einer Reihe von Anforderungen, die auf regulatorischen Rahmenbedingungen, branchenüblichen Best Practices oder Unternehmensrichtlinien basieren. Security Hub CSPM ordnet diese Anforderungen den Kontrollen zu und führt Sicherheitsüberprüfungen der Kontrollen durch, um zu beurteilen, ob die Anforderungen eines Standards erfüllt werden. Jeder Standard umfasst mehrere Kontrollen.

Security Hub CSPM unterstützt derzeit die folgenden Standards:

- **AWS Bewährte grundlegende Sicherheitsverfahren** — Dieser Standard wurde von Branchenexperten entwickelt AWS und ist eine Zusammenstellung von bewährten Sicherheitsmethoden für Unternehmen, unabhängig von Branche oder Größe. Er bietet eine Reihe von Kontrollen, die erkennen, wenn Sie AWS-Konten und Ihre Ressourcen von den bewährten Sicherheitsmethoden abweichen. Es enthält auch präskriptive Anleitungen zur Verbesserung und Aufrechterhaltung Ihrer Sicherheitslage.

- **AWS Resource Tagging** — Mit diesem von Security Hub CSPM entwickelten Standard können Sie feststellen, ob Ihre AWS Ressourcen über Tags verfügen. Ein Tag ist ein Schlüssel-Wert-Paar, das als Metadaten für eine Ressource fungiert. AWS Mithilfe von Tags können Sie Ressourcen identifizieren, kategorisieren, verwalten und nach ihnen suchen. AWS Sie können beispielsweise Tags verwenden, um Ressourcen nach Zweck, Eigentümer oder Umgebung zu kategorisieren.
- **CIS AWS Foundations Benchmark** — Dieser vom Center for Internet Security (CIS) entwickelte Standard bietet sichere Konfigurationsrichtlinien für AWS. Er legt eine Reihe von Richtlinien und bewährten Methoden zur Sicherheitskonfiguration für eine Untergruppe von AWS-Services Ressourcen fest, wobei der Schwerpunkt auf grundlegenden, testbaren und architekturunabhängigen Einstellungen liegt. Die Richtlinien beinhalten klare Implementierungs- und step-by-step Bewertungsverfahren.
- **NIST SP 800-53 Revision 5** — Dieser Standard entspricht den Anforderungen des National Institute of Standards and Technology (NIST) zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationssystemen und kritischen Ressourcen. Der zugehörige Rahmen gilt im Allgemeinen für US-Bundesbehörden oder Organisationen, die mit US-Bundesbehörden oder Informationssystemen zusammenarbeiten. Private Organisationen können die Anforderungen jedoch auch als Richtschnur verwenden.
- **NIST SP 800-171 Revision 2** — Dieser Standard entspricht den Sicherheitsempfehlungen und -anforderungen des NIST zum Schutz der Vertraulichkeit kontrollierter, nicht klassifizierter Informationen (CUI) in Systemen und Organisationen, die nicht Teil der US-Bundesregierung sind. CUI sind Informationen, die die staatlichen Klassifizierungskriterien nicht erfüllen, aber als sensibel gelten und von der US-Bundesregierung oder anderen Stellen im Auftrag der US-Bundesregierung erstellt oder in Besitz genommen werden.
- **PCI DSS** — Dieser Standard entspricht dem vom PCI Security Standards Council (SSC) definierten Compliance-Framework für den Payment Card Industry Data Security Standard (PCI DSS). Das Framework enthält eine Reihe von Regeln und Richtlinien für den sicheren Umgang mit Kredit- und Debitkarteninformationen. Das Framework gilt im Allgemeinen für Organisationen, die Karteninhaberdaten speichern, verarbeiten oder übertragen.
- **Service-verwalteter Standard, AWS Control Tower** — Dieser Standard hilft Ihnen bei der Konfiguration der proaktiven Kontrollen, die AWS Control Tower neben den detektiven Kontrollen von Security Hub CSPM bereitgestellt werden. AWS Control Tower bietet eine einfache Möglichkeit, eine Umgebung mit AWS mehreren Konten einzurichten und zu verwalten und dabei die vorgeschriebenen Best Practices zu befolgen. Indem Sie sowohl proaktive als auch detektive Kontrollen für Ihre AWS Umgebung aktivieren, können Sie Ihr Sicherheitsniveau in verschiedenen Entwicklungsphasen verbessern.

Die CSPM-Standards und -Kontrollen von Security Hub garantieren nicht die Einhaltung gesetzlicher Rahmenbedingungen oder Audits. Stattdessen bieten sie eine Möglichkeit, den Zustand Ihrer Ressourcen und Ihrer Ressourcen zu bewerten AWS-Konten und zu überwachen. Wir empfehlen, jeden Standard zu aktivieren, der für Ihre Geschäftsanforderungen, Ihre Branche oder Ihren Anwendungsfall relevant ist.

Einzelne Kontrollen können für mehr als einen Standard gelten. Wenn Sie mehrere Standards aktivieren, empfehlen wir, auch konsolidierte Kontrollergebnisse zu aktivieren. Wenn Sie dies tun, generiert Security Hub CSPM einen einzigen Befund für jedes Steuerelement, auch wenn das Steuerelement für mehr als einen Standard gilt. Wenn Sie konsolidierte Kontrollergebnisse nicht aktivieren, generiert Security Hub CSPM für jeden aktivierten Standard, für den eine Kontrolle gilt, einen separaten Befund. Wenn Sie beispielsweise zwei Standards aktivieren und eine Kontrolle für beide gilt, erhalten Sie zwei separate Ergebnisse für die Kontrolle, einen für jeden Standard. Wenn Sie konsolidierte Kontrollergebnisse aktivieren, erhalten Sie nur ein Ergebnis für die Kontrolle. Weitere Informationen finden Sie unter [Konsolidierte Kontrollergebnisse](#).

Detaillierte Referenz standardmäßig

- [AWS Standard für grundlegende Best Practices im Bereich Sicherheit im Security Hub CSPM](#)
- [AWS Standard für Ressourcen-Tagging in Security Hub CSPM](#)
- [Benchmark der AWS GUS-Stiftungen im Security Hub CSPM](#)
- [NIST SP 800-53 Revision 5 im Security Hub CSPM](#)
- [NIST SP 800-171 Revision 2 im Security Hub CSPM](#)
- [PCI DSS im Security Hub CSPM](#)
- [Von Diensten verwaltete Standards in Security Hub CSPM](#)

AWS Standard für grundlegende Best Practices im Bereich Sicherheit im Security Hub CSPM

Der von AWS Branchenexperten entwickelte Standard AWS Foundational Security Best Practices (FSBP) ist eine Zusammenstellung von bewährten Sicherheitsmethoden für Unternehmen, unabhängig von Branche oder Größe. Er bietet eine Reihe von Kontrollen, die erkennen, wann AWS-Konten und welche Ressourcen von den bewährten Sicherheitsmethoden abweichen. Es enthält auch präskriptive Leitlinien zur Verbesserung und Aufrechterhaltung der Sicherheitslage Ihres Unternehmens.

In AWS Security Hub Cloud Security Posture Management (CSPM) umfasst der Standard AWS Foundational Security Best Practices Kontrollen, mit denen Sie AWS-Konten und Ihre Workloads kontinuierlich bewertet werden und Sie dabei unterstützen, Bereiche zu identifizieren, die von den bewährten Sicherheitsmethoden abweichen. Die Kontrollen beinhalten bewährte Sicherheitsverfahren für Ressourcen aus mehreren Ländern. AWS-Services Jedem Steuerelement wird eine Kategorie zugewiesen, die die Sicherheitsfunktion widerspiegelt, für die das Steuerelement gilt. Eine Liste der Kategorien und weitere Informationen finden Sie unter [Kontrollkategorien](#).

Kontrollen, die für den Standard gelten

In der folgenden Liste wird angegeben, welche AWS Security Hub Cloud Security Posture Management (CSPM) -Kontrollen für den Standard AWS Foundational Security Best Practices (v1.0.0) gelten. Um die Details einer Kontrolle zu überprüfen, wählen Sie die Steuerung aus.

[\[Account.1\] Sicherheitskontaktinformationen sollten bereitgestellt werden für AWS-Konto](#)

[\[ACM.1\] Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden](#)

[\[ACM.2\] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden](#)

[\[APIGateway.1\] API Gateway REST und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein](#)

[\[APIGateway.2\] API Gateway REST API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden](#)

[\[APIGateway.3\] Bei den REST-API-Stufen von API Gateway sollte die AWS X-Ray Ablaufverfolgung aktiviert sein](#)

[\[APIGateway.4\] API Gateway sollte mit einer WAF-Web-ACL verknüpft sein](#)

[\[APIGateway.5\] API Gateway REST API-Cache-Daten sollten im Ruhezustand verschlüsselt werden](#)

[\[APIGateway.8\] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben](#)

[\[APIGateway.9\] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein](#)

[\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)

[\[AppSync.2\] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben](#)

[\[AppSync.5\] AWS AppSync GraphQL APIs sollte nicht mit API-Schlüsseln authentifiziert werden](#)

[\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)

[\[Athena.4\] Bei Athena-Arbeitsgruppen sollte die Protokollierung aktiviert sein](#)

[\[AutoScaling.1\] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden](#)

[\[AutoScaling.2\] Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken](#)

[\[AutoScaling.3\] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2 Instances so konfigurieren, dass sie Instance Metadata Service Version 2 \(IMDSv2\) benötigen](#)

[\[Autoscaling.5\] EC2 Amazon-Instances, die mit Auto Scaling Scaling-Gruppenstartkonfigurationen gestartet wurden, sollten keine öffentlichen IP-Adressen haben](#)

[\[AutoScaling.6\] Auto Scaling Scaling-Gruppen sollten mehrere Instance-Typen in mehreren Availability Zones verwenden](#)

[\[AutoScaling.9\] Amazon EC2 Auto Scaling Scaling-Gruppen sollten EC2 Amazon-Startvorlagen verwenden](#)

[\[Backup.1\] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein](#)

[Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)

[\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)

[\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)

[\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)

[\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)

[\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)

[\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)

[\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)

[\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)

[\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)

[\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)

[\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)

[\[CloudTrail.1\] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst](#)

[\[CloudTrail.2\] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben](#)

[\[CloudTrail.4\] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein](#)

[\[CloudTrail.5\] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden](#)

[\[CodeBuild.1\] Das CodeBuild Bitbucket-Quell-Repository URLs sollte keine vertraulichen Anmeldeinformationen enthalten](#)

[\[CodeBuild.2\] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten](#)

[\[CodeBuild.3\] CodeBuild S3-Protokolle sollten verschlüsselt sein](#)

[\[CodeBuild.4\] CodeBuild Projektumgebungen sollten eine AWS Config Protokollierungsdauer haben](#)

[\[CodeBuild.7\] Exporte von CodeBuild Berichtsgruppen sollten im Ruhezustand verschlüsselt werden](#)

[\[Cognito.2\] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen](#)

[\[Config.1\] AWS Config sollte aktiviert sein und die serviceverknüpfte Rolle für die Ressourcenaufzeichnung verwenden](#)

[\[Connect.2\] Für Amazon Connect Connect-Instances sollte die Protokollierung aktiviert sein](#)
[CloudWatch](#)

[\[DataFirehose.1\] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden](#)

[\[DataSync.1\] Für DataSync Aufgaben sollte die Protokollierung aktiviert sein](#)

[\[DMS.1\] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein](#)

[\[DMS.6\] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein](#)

[\[DMS.7\] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein](#)

[\[DMS.8\] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein](#)

[\[DMS.9\] DMS-Endpunkte sollten SSL verwenden](#)

[\[DMS.10\] Bei DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein](#)

[\[DMS.11\] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein](#)

[\[DMS.12\] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein](#)

[\[DocumentDB.1\] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden](#)

[\[DocumentDB.2\] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen](#)

[\[DocumentDB.3\] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein](#)

[\[DocumentDB.4\] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen](#)
[CloudWatch](#)

[\[DocumentDB.5\] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein](#)

[\[DocumentDB.6\] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden](#)

[\[DynamoDB.1\] DynamoDB-Tabellen sollten die Kapazität automatisch bei Bedarf skalieren](#)

[\[DynamoDB.2\] Bei DynamoDB-Tabellen sollte die Wiederherstellung aktiviert sein point-in-time](#)

[\[DynamoDB.3\] DynamoDB Accelerator \(DAX\) -Cluster sollten im Ruhezustand verschlüsselt werden](#)

[\[DynamoDB.6\] Bei DynamoDB-Tabellen sollte der Löschschutz aktiviert sein](#)

[\[DynamoDB.7\] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden](#)

[\[EC2.1\] Amazon EBS-Snapshots sollten nicht öffentlich wiederherstellbar sein](#)

[\[EC2.2\] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen](#)

[\[EC2.3\] Angehängte Amazon EBS-Volumes sollten im Ruhezustand verschlüsselt werden](#)

[\[EC2.4\] Gestoppte EC2 Instances sollten nach einem bestimmten Zeitraum entfernt werden](#)

[\[EC2.6\] Die VPC-Flow-Protokollierung sollte in allen aktiviert sein VPCs](#)

[\[EC2.7\] Die EBS-Standardverschlüsselung sollte aktiviert sein](#)

[\[EC2.8\] EC2 Instances sollten Instance Metadata Service Version 2 \(\) verwenden IMDSv2](#)

[\[EC2.9\] EC2 Amazon-Instances sollten keine öffentliche IPv4 Adresse haben](#)

[\[EC2.10\] Amazon EC2 sollte so konfiguriert sein, dass es VPC-Endpunkte verwendet, die für den Amazon-Service erstellt wurden EC2](#)

[\[EC2.15\] EC2 Amazon-Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen](#)

[\[EC2.16\] Ungenutzte Network Access Control Lists sollten entfernt werden](#)

[\[EC2.17\] EC2 Amazon-Instances sollten nicht mehrere verwenden ENIs](#)

[\[EC2.18\] Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Datenverkehr für autorisierte Ports zulassen](#)

[\[EC2.19\] Sicherheitsgruppen sollten keinen uneingeschränkten Zugriff auf Ports mit hohem Risiko zulassen](#)

[\[EC2.20\] Beide VPN-Tunnel für eine AWS Site-to-Site VPN-Verbindung sollten aktiv sein](#)

[\[EC2.21\] Das Netzwerk ACLs sollte keinen Zugang von 0.0.0.0/0 zu Port 22 oder Port 3389 zulassen](#)

[\[EC2.23\] Amazon EC2 Transit Gateways sollte VPC-Anhangsanfragen nicht automatisch akzeptieren](#)

[\[EC2.24\] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden](#)

[\[EC2.25\] EC2 Amazon-Startvorlagen sollten Netzwerkschnittstellen nicht öffentlich IPs zuweisen](#)

[\[EC2.51\] EC2 Client-VPN-Endpunkte sollten die Client-Verbindungsprotokollierung aktiviert haben](#)

[\[EC2.55\] VPCs sollte mit einem Schnittstellenendpunkt für die ECR-API konfiguriert werden](#)

[\[EC2.56\] VPCs sollte mit einem Schnittstellenendpunkt für Docker Registry konfiguriert werden](#)

[\[EC2.57\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager konfiguriert werden](#)

[\[EC2.58\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert sein](#)

[\[EC2.60\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden](#)

[\[EC2.170\] EC2 Startvorlagen sollten Instance Metadata Service Version 2 \(\) verwenden IMDSv2](#)

[\[EC2.171\] Bei EC2 VPN-Verbindungen sollte die Protokollierung aktiviert sein](#)

[\[EC2.172\] Die Einstellungen von EC2 VPC Block Public Access sollten den Internet-Gateway-Verkehr blockieren](#)

[\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)

[\[EC2.180\] Bei EC2 Netzwerkschnittstellen sollte die source/destination Überprüfung aktiviert sein](#)

[\[ECR.1\] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein](#)

[\[ECR.2\] Bei privaten ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein](#)

[\[ECR.3\] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein](#)

[\[ECS.1\] Amazon ECS-Aufgabendefinitionen sollten sichere Netzwerkmodi und Benutzerdefinitionen enthalten](#)

[\[ECS.2\] ECS-Diensten sollten nicht automatisch öffentliche IP-Adressen zugewiesen werden](#)

[\[ECS.3\] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen](#)

[\[ECS.4\] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden](#)

[\[ECS.5\] ECS-Container sollten auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sein](#)

[\[ECS.8\] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden](#)

[\[ECS.9\] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen](#)

[\[ECS.10\] Die ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen](#)

[\[ECS.12\] ECS-Cluster sollten Container Insights verwenden](#)

[\[ECS.16\] ECS-Aufgabensätze sollten öffentliche IP-Adressen nicht automatisch zuweisen](#)

[\[EFS.1\] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS](#)

[\[EFS.2\] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein](#)

[\[EFS.3\] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen](#)

[\[EFS.4\] EFS-Zugangspunkte sollten eine Benutzeridentität erzwingen](#)

[\[EFS.6\] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden](#)

[\[EFS.7\] Bei EFS-Dateisystemen sollten automatische Backups aktiviert sein](#)

[\[EFS.8\] EFS-Dateisysteme sollten im Ruhezustand verschlüsselt werden](#)

[\[EKS.1\] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein](#)

[\[EKS.2\] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden](#)

[\[EKS.3\] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden](#)

[\[EKS.8\] Bei EKS-Clustern sollte die Auditprotokollierung aktiviert sein](#)

[Bei \[ElastiCache.1\] ElastiCache \(Redis OSS\) -Clustern sollten automatische Backups aktiviert sein](#)

[\[ElastiCache.2\] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein](#)

[\[ElastiCache.3\] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein](#)

[\[ElastiCache.4\] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden](#)

[\[ElastiCache.5\] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden](#)

[\[ElastiCache.6\] Für Replikationsgruppen ElastiCache \(Redis OSS\) früherer Versionen sollte Redis OSS AUTH aktiviert sein](#)

[\[ElastiCache.7\] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden](#)

[\[ElasticBeanstalk.1\] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben](#)

[\[ElasticBeanstalk.2\] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein](#)

[\[ElasticBeanstalk.3\] Elastic Beanstalk sollte Logs streamen nach CloudWatch](#)

[\[ELB.1\] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden](#)

[\[ELB.2\] Classic Load Balancer mit SSL/HTTPS Listnern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager](#)

[\[ELB.3\] Classic Load Balancer Balancer-Listener sollten mit HTTPS- oder TLS-Terminierung konfiguriert werden](#)

[\[ELB.4\] Application Load Balancer sollte so konfiguriert sein, dass ungültige HTTP-Header gelöscht werden](#)

[\[ELB.5\] Die Protokollierung von Anwendungen und Classic Load Balancers sollte aktiviert sein](#)

[\[ELB.6\] Für Anwendungen, Gateways und Network Load Balancers sollte der Löschschutz aktiviert sein](#)

[\[ELB.7\] Bei Classic Load Balancers sollte der Verbindungsabbau aktiviert sein](#)

[\[ELB.8\] Classic Load Balancer mit SSL-Listnern sollten eine vordefinierte Sicherheitsrichtlinie mit starker Dauer verwenden AWS Config](#)

[\[ELB.9\] Bei Classic Load Balancers sollte der zonenübergreifende Load Balancing aktiviert sein](#)

[\[ELB.10\] Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken](#)

[\[ELB.12\] Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden](#)

[\[ELB.13\] Anwendungs-, Netzwerk- und Gateway-Load Balancer sollten sich über mehrere Availability Zones erstrecken](#)

[\[ELB.14\] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden](#)

[\[ELB.17\] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden](#)

[\[ELB.18\] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln](#)

[\[EMR.1\] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben](#)

[\[EMR.2\] Die Amazon EMR-Einstellung zum Blockieren des öffentlichen Zugriffs sollte aktiviert sein](#)

[\[EMR.3\] Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden](#)

[\[EMR.4\] Amazon EMR-Sicherheitskonfigurationen sollten bei der Übertragung verschlüsselt werden](#)

[\[ES.1\] Bei Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein](#)

[\[ES.2\] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein](#)

[\[ES.3\] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden](#)

[\[ES.4\] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein](#)

[\[ES.5\] Für Elasticsearch-Domains sollte die Audit-Protokollierung aktiviert sein](#)

[\[ES.6\] Elasticsearch-Domains sollten mindestens drei Datenknoten haben](#)

[\[ES.7\] Elasticsearch-Domänen sollten mit mindestens drei dedizierten Master-Knoten konfiguriert werden](#)

[\[ES.8\] Verbindungen zu Elasticsearch-Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden](#)

[\[EventBridge.3\] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden](#)

[FSx.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden

[FSx.2] FSx für Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden

[FSx.3] FSx für OpenZFS-Dateisysteme sollte für die Multi-AZ-Bereitstellung konfiguriert werden

[FSx.4] FSx für NetApp ONTAP-Dateisysteme sollte für die Multi-AZ-Bereitstellung konfiguriert sein

[FSx.5] FSx für Windows-Dateiserver sollten für die Multi-AZ-Bereitstellung konfiguriert sein

[Glue.3] Transformationen für AWS Glue maschinelles Lernen sollten im Ruhezustand verschlüsselt werden

[Glue.4] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue

[GuardDuty.1] GuardDuty sollte aktiviert sein

[GuardDuty.5] GuardDuty EKS Audit Log Monitoring sollte aktiviert sein

[GuardDuty.6] GuardDuty Lambda Protection sollte aktiviert sein

[GuardDuty.7] GuardDuty EKS Runtime Monitoring sollte aktiviert sein

[GuardDuty.8] Der GuardDuty Malware-Schutz für EC2 sollte aktiviert sein

[GuardDuty.9] Der GuardDuty RDS-Schutz sollte aktiviert sein

[GuardDuty.10] Der GuardDuty S3-Schutz sollte aktiviert sein

[GuardDuty.11] GuardDuty Runtime Monitoring sollte aktiviert sein

[GuardDuty.12] GuardDuty ECS Runtime Monitoring sollte aktiviert sein

[GuardDuty.13] GuardDuty EC2 Runtime Monitoring sollte aktiviert sein

[IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen

[IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein

[IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden

[\[IAM.4\] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren](#)

[\[IAM.5\] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen](#)

[\[IAM.6\] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.](#)

[\[IAM.7\] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein](#)

[\[IAM.8\] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden](#)

[\[IAM.21\] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen](#)

[\[Inspector.1\] Das EC2 Scannen mit Amazon Inspector sollte aktiviert sein](#)

[\[Inspector.2\] Das Amazon Inspector ECR-Scannen sollte aktiviert sein](#)

[\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)

[\[Inspector.4\] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein](#)

[\[Kinesis.1\] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden](#)

[\[Kinesis.3\] Kinesis-Streams sollten über eine angemessene Aufbewahrungsfrist für Daten verfügen](#)

[\[KMS.1\] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)

[\[KMS.2\] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)

[\[KMS.3\] AWS KMS keys sollte nicht unbeabsichtigt gelöscht werden](#)

[\[KMS.5\] KMS-Schlüssel sollten nicht öffentlich zugänglich sein](#)

[\[Lambda.1\] Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten](#)

[\[Lambda.2\] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden](#)

[\[Lambda.5\] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren](#)

[\[Macie.1\] Amazon Macie sollte aktiviert sein](#)

[\[Macie.2\] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein](#)

[\[MQ.2\] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch](#)

[\[MQ.3\] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein](#)

[\[MSK.1\] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden](#)

[\[MSK.3\] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden](#)

[\[MSK.4\] Bei MSK-Clustern sollte der öffentliche Zugriff deaktiviert sein](#)

[\[MSK.5\] Bei MSK-Konnektoren sollte die Protokollierung aktiviert sein](#)

[\[MSK.6\] MSK-Cluster sollten den nicht authentifizierten Zugriff deaktivieren](#)

[\[Neptune.1\] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden](#)

[\[Neptune.2\] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)

[\[Neptune.3\] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein](#)

[\[Neptune.4\] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein](#)

[\[Neptune.5\] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein](#)

[\[Neptune.6\] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden](#)

[\[Neptune.7\] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein](#)

[\[Neptune.8\] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren](#)

[\[NetworkFirewall.2\] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein](#)

[\[NetworkFirewall.3\] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet haben](#)

[\[NetworkFirewall.4\] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ sein.](#)

[\[NetworkFirewall.5\] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ sein.](#)

[\[NetworkFirewall.6\] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein](#)

[\[NetworkFirewall.9\] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein](#)

[\[NetworkFirewall.10\] Bei Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein](#)

[Bei \[Opensearch.1\] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein](#)

[\[Opensearch.2\] OpenSearch -Domains sollten nicht öffentlich zugänglich sein](#)

[\[Opensearch.3\] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden](#)

[Die Protokollierung von \[Opensearch.4\] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein](#)

[Für \[Opensearch.5\] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein](#)

[\[Opensearch.6\] OpenSearch Domains sollten mindestens drei Datenknoten haben](#)

[Für \[Opensearch.7\] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein](#)

[\[Opensearch.8\] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden](#)

[Auf \[Opensearch.10\] OpenSearch -Domains sollte das neueste Softwareupdate installiert sein](#)

[\[PCA.1\] AWS Private CA Root-Zertifizierungsstelle sollte deaktiviert sein](#)

[\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)

[\[RDS.1\] Der RDS-Snapshot sollte privat sein](#)

[\[RDS.2\] RDS-DB-Instances sollten, wie in der Konfiguration festgelegt, den öffentlichen Zugriff verbieten PubliclyAccessible](#)

[\[RDS.3\] Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein.](#)

[\[RDS.4\] RDS-Cluster-Snapshots und Datenbank-Snapshots sollten im Ruhezustand verschlüsselt werden](#)

[\[RDS.5\] RDS-DB-Instances sollten mit mehreren Availability Zones konfiguriert werden](#)

- [\[RDS.6\] Die erweiterte Überwachung sollte für RDS-DB-Instances konfiguriert werden](#)
- [\[RDS.7\] Bei RDS-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[RDS.8\] Für RDS-DB-Instances sollte der Löschschutz aktiviert sein](#)
- [\[RDS.9\] RDS-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[RDS.10\] Die IAM-Authentifizierung sollte für RDS-Instances konfiguriert werden](#)
- [\[RDS.11\] Bei RDS-Instances sollten automatische Backups aktiviert sein](#)
- [\[RDS.12\] Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden](#)
- [\[RDS.13\] Automatische RDS-Upgrades für Nebenversionen sollten aktiviert sein](#)
- [\[RDS.14\] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein](#)
- [\[RDS.15\] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden](#)
- [\[RDS.16\] Aurora-DB-Cluster sollten so konfiguriert sein, dass sie Tags in DB-Snapshots kopieren](#)
- [\[RDS.17\] RDS-DB-Instances sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren](#)
- [\[RDS.19\] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Cluster-Ereignisse konfiguriert werden](#)
- [\[RDS.20\] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Ereignisse der Datenbankinstanz konfiguriert werden](#)
- [\[RDS.21\] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbankparametergruppenereignisse konfiguriert werden](#)
- [\[RDS.22\] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbanksicherheitsgruppenereignisse konfiguriert werden](#)
- [\[RDS.23\] RDS-Instances sollten keinen Standard-Port für die Datenbank-Engine verwenden](#)
- [\[RDS.24\] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden](#)
- [\[RDS.25\] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden](#)

[\[RDS.27\] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden](#)

[\[RDS.34\] Aurora MySQL-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)

[\[RDS.35\] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein](#)

[\[RDS.36\] RDS für PostgreSQL-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch](#)

[\[RDS.37\] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch](#)

[\[RDS.40\] RDS für SQL Server-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch](#)

[\[RDS.41\] RDS für SQL Server-DB-Instances sollten bei der Übertragung verschlüsselt werden](#)

[\[RDS.42\] RDS für MariaDB-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch](#)

[\[RDS.44\] RDS für MariaDB-DB-Instances sollte bei der Übertragung verschlüsselt werden](#)

[\[RDS.45\] Bei Aurora MySQL-DB-Clustern sollte die Audit-Protokollierung aktiviert sein](#)

[\[Redshift.1\] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten](#)

[\[Redshift.2\] Verbindungen zu Amazon Redshift Redshift-Clustern sollten bei der Übertragung verschlüsselt werden](#)

[\[Redshift.3\] Bei Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein](#)

[\[Redshift.4\] Bei Amazon Redshift Redshift-Clustern sollte die Auditprotokollierung aktiviert sein](#)

[\[Redshift.6\] Bei Amazon Redshift sollten automatische Upgrades auf Hauptversionen aktiviert sein](#)

[\[Redshift.7\] Redshift-Cluster sollten erweitertes VPC-Routing verwenden](#)

[\[Redshift.8\] Amazon Redshift Redshift-Cluster sollten nicht den standardmäßigen Admin-Benutzernamen verwenden](#)

[\[Redshift.9\] Redshift-Cluster sollten nicht den Standard-Datenbanknamen verwenden](#)

[\[Redshift.10\] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden](#)

[\[Redshift.15\] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen](#)

[\[Redshift.18\] Für Redshift-Cluster sollten Multi-AZ-Bereitstellungen aktiviert sein](#)

[\[RedshiftServerless.1\] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden](#)

[\[RedshiftServerless.2\] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein](#)

[\[RedshiftServerless.3\] Serverlose Redshift-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten](#)

[\[RedshiftServerless.5\] Redshift Serverless-Namespaces sollten nicht den Standard-Admin-Benutzernamen verwenden](#)

[\[RedshiftServerless.6\] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch](#)

[\[RedshiftServerless.7\] Redshift Serverless-Namespaces sollten nicht den Standard-Datenbanknamen verwenden](#)

[\[S3.1\] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein](#)

[\[S3.2\] S3-Allzweck-Buckets sollten den öffentlichen Lesezugriff blockieren](#)

[\[S3.3\] S3-Allzweck-Buckets sollten den öffentlichen Schreibzugriff blockieren](#)

[\[S3.5\] S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erfordern](#)

[\[S3.6\] Allgemeine S3-Bucket-Richtlinien sollten den Zugriff auf andere einschränken AWS-Konten](#)

[\[S3.8\] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren](#)

[\[S3.9\] Bei S3-Allzweck-Buckets sollte die Serverzugriffsprotokollierung aktiviert sein](#)

[\[S3.12\] ACLs sollte nicht zur Verwaltung des Benutzerzugriffs auf S3-Allzweck-Buckets verwendet werden](#)

[\[S3.13\] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben](#)

[\[S3.19\] Bei S3-Zugriffspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein](#)

[S3.24] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein

[S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben

[SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben

[SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden

[SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben

[SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein

[SageMaker.5] SageMaker Modelle sollten eingehenden Datenverkehr blockieren

[SageMaker.8] SageMaker Notebook-Instances sollten auf unterstützten Plattformen laufen

[SecretsManager.1] Bei Secrets Manager Manager-Geheimnissen sollte die automatische Rotation aktiviert sein

[SecretsManager.2] Secrets Manager Manager-Geheimnisse, die mit automatischer Rotation konfiguriert sind, sollten erfolgreich rotieren

[SecretsManager.3] Unbenutzte Secrets Manager Manager-Geheimnisse entfernen

[SecretsManager.4] Secrets Manager Manager-Geheimnisse sollten innerhalb einer bestimmten Anzahl von Tagen rotiert werden

[ServiceCatalog.1] Servicecatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden

[SNS.4] Zugriffsrichtlinien für SNS-Themen sollten keinen öffentlichen Zugriff zulassen

[SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt werden

[SQS.3] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen

[SSM.1] EC2 Amazon-Instances sollten verwaltet werden von AWS Systems Manager

[SSM.2] Von Systems Manager verwaltete EC2 Amazon-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben

[SSM.3] Von Systems Manager verwaltete EC2 Amazon-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben

[SSM.4] SSM-Dokumente sollten nicht öffentlich sein

[SSM.6] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch

[SSM.7] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein

[StepFunctions.1] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben

[Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden

[Transfer.3] Bei Connectoren der Transfer-Familie sollte die Protokollierung aktiviert sein

[WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein

[WAF.2] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung haben

[WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben

[WAF.4] AWS WAF Classic Regional Web ACLs sollte mindestens eine Regel oder Regelgruppe enthalten

[WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben

[WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben

[WAF.8] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben

[WAF.10] AWS WAF web ACLs sollte mindestens eine Regel oder Regelgruppe haben

Für [WAF.12] AWS WAF Regeln sollten Metriken aktiviert sein CloudWatch

[WorkSpaces.1] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden

[\[WorkSpaces.2\] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden](#)

AWS Standard für Ressourcen-Tagging in Security Hub CSPM

Mit dem AWS Resource Tagging-Standard, der von AWS Security Hub Cloud Security Posture Management (CSPM) entwickelt wurde, können Sie feststellen, ob in Ihren AWS Ressourcen Tags fehlen. Tags sind Schlüssel-Wert-Paare, die als Metadaten für die Organisation von Ressourcen dienen. AWS Bei den meisten AWS Ressourcen haben Sie die Möglichkeit, einer Ressource Tags hinzuzufügen, wenn Sie die Ressource erstellen oder nachdem Sie die Ressource erstellt haben. Zu den Ressourcen gehören beispielsweise CloudFront Amazon-Distributionen, Amazon Elastic Compute Cloud (Amazon EC2) -Instances und Secrets in AWS Secrets Manager. Mithilfe von Tags können Sie AWS Ressourcen verwalten, identifizieren, organisieren, suchen und filtern.

Jedes Tag besteht aus zwei Teilen:

- Ein Tag-Schlüssel, zum Beispiel, CostCenterEnvironment, oder. Project Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.
- Ein Tag-Wert, zum Beispiel oder. 111122223333 Production Wie bei Tag-Schlüsseln wird auch bei Tag-Werten zwischen Groß- und Kleinschreibung unterschieden.

Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Informationen zum Hinzufügen von Tags zu AWS Ressourcen finden Sie im Benutzerhandbuch [Tagging AWS Resources and Tag Editor](#).

Für jedes Steuerelement, das für den AWS Resource Tagging-Standard in Security Hub CSPM gilt, können Sie optional den unterstützten Parameter verwenden, um Tag-Schlüssel anzugeben, nach denen das Steuerelement suchen soll. Wenn Sie keine Tag-Schlüssel angeben, prüft das Steuerelement nur, ob mindestens ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn eine Ressource keine Tag-Schlüssel hat.

Bevor Sie den AWS Resource Tagging-Standard aktivieren, müssen Sie zunächst die Ressourcenaufzeichnung aktivieren und konfigurieren. AWS Config Achten Sie bei der Konfiguration der Ressourcenaufzeichnung auch darauf, sie für alle AWS Ressourcentypen zu aktivieren, die durch die für den Standard geltenden Kontrollen überprüft werden. Andernfalls ist Security Hub CSPM möglicherweise nicht in der Lage, die geeigneten Ressourcen zu bewerten und genaue Ergebnisse für Kontrollen zu generieren, die für den Standard gelten. Weitere Informationen, einschließlich einer Liste der aufzuzeichnenden Ressourcentypen, finden Sie unter. [Erforderliche AWS Config Ressourcen für Kontrollbefunde](#)

 Note

Der AWS Resource Tagging-Standard ist in Kanada, West (Calgary), China und AWS GovCloud (US) Regionen nicht verfügbar.

Nachdem Sie den AWS Resource Tagging-Standard aktiviert haben, erhalten Sie erste Ergebnisse für Kontrollen, die für den Standard gelten. Beachten Sie, dass es bis zu 18 Stunden dauern kann, bis Security Hub CSPM Ergebnisse für Kontrollen generiert, die dieselbe AWS Config serviceverknüpfte Regel verwenden wie Kontrollen, die für andere aktivierte Standards gelten. Weitere Informationen finden Sie unter [Zeitplan für die Ausführung von Sicherheitsprüfungen](#).

Der AWS Resource Tagging-Standard hat den folgenden Amazon-Ressourcennamen (ARN): `arn:aws:securityhub:region::standards/aws-resource-tagging-standard/v/1.0.0`. Sie können auch den [GetEnabledStandards](#) Betrieb der Security Hub CSPM-API verwenden, um den ARN eines aktivierten Standards zu ermitteln.

Kontrollen, die für den Standard gelten

Die folgende Liste gibt an, welche AWS Security Hub Cloud Security Posture Management (CSPM) -Steuerelemente für den AWS Resource Tagging-Standard (v1.0.0) gelten. Um die Details eines Steuerelements zu überprüfen, wählen Sie das Steuerelement aus.

- [\[ACM.3\] ACM-Zertifikate sollten mit einem Tag versehen werden](#)
- [\[Amplify.1\] Amplify-Apps sollten markiert werden](#)
- [\[Amplify.2\] Amplify-Zweige sollten markiert werden](#)
- [\[AppConfig.1\] AWS AppConfig Anwendungen sollten markiert werden](#)
- [\[AppConfig.2\] AWS AppConfig Konfigurationsprofile sollten mit Tags versehen werden](#)
- [\[AppConfig.3\] AWS AppConfig Umgebungen sollten markiert werden](#)
- [\[AppConfig.4\] AWS AppConfig Erweiterungszuordnungen sollten markiert werden](#)
- [\[AppFlow.1\] AppFlow Amazon-Datenflüsse sollten mit Tags versehen werden](#)
- [\[AppRunner.1\] App Runner-Dienste sollten markiert sein](#)
- [\[AppRunner.2\] App Runner VPC-Konnektoren sollten markiert sein](#)
- [\[AppSync.4\] AWS AppSync GraphQL APIs sollte markiert sein](#)
- [\[Athena.2\] Athena-Datenkataloge sollten mit Tags versehen werden](#)

- [\[Athena.3\] Athena-Arbeitsgruppen sollten markiert werden](#)
- [\[AutoScaling.10\] EC2 Auto Scaling Scaling-Gruppen sollten markiert werden](#)
- [\[Backup.2\] AWS Backup Wiederherstellungspunkte sollten markiert werden](#)
- [\[Backup.3\] AWS Backup Tresore sollten markiert sein](#)
- [\[Backup.4\] AWS Backup Berichtspläne sollten markiert werden](#)
- [\[Backup.5\] AWS Backup Backup-Pläne sollten markiert werden](#)
- [\[Batch.1\] Warteschlangen für Batch-Jobs sollten markiert werden](#)
- [\[Batch.2\] Richtlinien für die Batch-Planung sollten gekennzeichnet sein](#)
- [\[Batch.3\] Batch-Computing-Umgebungen sollten markiert werden](#)
- [\[Batch.4\] Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden](#)
- [\[CloudFormation.2\] CloudFormation Stapel sollten markiert werden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudTrail.9\] CloudTrail Pfade sollten markiert werden](#)
- [\[CodeArtifact.1\] CodeArtifact Repositorien sollten mit Tags versehen werden](#)
- [\[CodeGuruProfiler.1\] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden](#)
- [\[CodeGuruReviewer.1\] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden](#)
- [\[Connect.1\] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden](#)
- [\[DataSync.2\] DataSync Aufgaben sollten mit Tags versehen werden](#)
- [\[Detective.1\] Verhaltensdiagramme von Detektiven sollten markiert werden](#)
- [\[DMS.2\] DMS-Zertifikate sollten gekennzeichnet sein](#)
- [\[DMS.3\] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden](#)
- [\[DMS.4\] DMS-Replikationsinstanzen sollten markiert werden](#)
- [\[DMS.5\] Subnetzgruppen für die DMS-Replikation sollten markiert werden](#)
- [\[DynamoDB.5\] DynamoDB-Tabellen sollten mit Tags versehen werden](#)
- [\[EC2.33\] EC2 Transit-Gateway-Anhänge sollten mit Tags versehen werden](#)
- [\[EC2.34\] Die Routentabellen für EC2 Transit-Gateways sollten mit Tags versehen werden](#)
- [\[EC2.35\] EC2 Netzwerkschnittstellen sollten markiert werden](#)
- [\[EC2.36\] EC2 Kunden-Gateways sollten mit Tags versehen werden](#)

- [\[EC2.37\] EC2 Elastische IP-Adressen sollten mit Tags versehen werden](#)
- [\[EC2.38\] EC2 Instances sollten markiert werden](#)
- [\[EC2.39\] EC2 Internet-Gateways sollten markiert werden](#)
- [\[EC2.40\] EC2 NAT-Gateways sollten markiert werden](#)
- [\[EC2.41\] Das EC2 Netzwerk ACLs sollte markiert sein](#)
- [\[EC2.42\] EC2 Routing-Tabellen sollten mit Tags versehen werden](#)
- [\[EC2.43\] EC2 Sicherheitsgruppen sollten markiert werden](#)
- [\[EC2.44\] EC2 Subnetze sollten markiert werden](#)
- [\[EC2.45\] EC2 Volumen sollten mit Tags versehen werden](#)
- [\[EC2.46\] Amazon VPCs sollte markiert werden](#)
- [\[EC2.47\] Amazon VPC Endpoint Services sollten markiert werden](#)
- [\[EC2.48\] Amazon VPC-Flow-Logs sollten mit Tags versehen werden](#)
- [\[EC2.49\] Amazon VPC-Peering-Verbindungen sollten markiert werden](#)
- [\[EC2.50\] EC2 VPN-Gateways sollten markiert werden](#)
- [\[EC2.52\] EC2 Transit-Gateways sollten markiert werden](#)
- [\[EC2.174\] EC2 DHCP-Optionssätze sollten mit Tags versehen werden](#)
- [\[EC2.175\] EC2 Startvorlagen sollten mit Tags versehen sein](#)
- [\[EC2.176\] EC2 Präfixlisten sollten mit Tags versehen werden](#)
- [\[EC2.177\] EC2 Traffic Mirror-Sitzungen sollten mit Tags versehen werden](#)
- [\[EC2.178\] Filter für EC2 Verkehrsspiegel sollten mit Tags versehen werden](#)
- [\[EC2.179\] EC2 Traffic-Spiegel-Ziele sollten markiert werden](#)
- [\[ECR.4\] Öffentliche ECR-Repositoryn sollten markiert werden](#)
- [\[ECS.13\] ECS-Services sollten markiert werden](#)
- [\[ECS.14\] ECS-Cluster sollten markiert werden](#)
- [\[ECS.15\] ECS-Aufgabendefinitionen sollten mit Tags versehen werden](#)
- [\[EFS.5\] EFS-Zugangspunkte sollten markiert werden](#)
- [\[EKS.6\] EKS-Cluster sollten markiert werden](#)
- [\[EKS.7\] Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden](#)
- [\[ES.9\] Elasticsearch-Domains sollten markiert werden](#)

- [\[EventBridge.2\] EventBridge Eventbusse sollten gekennzeichnet sein](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[Glue.1\] AWS Glue Jobs sollten markiert werden](#)
- [\[GuardDuty.2\] GuardDuty Filter sollten mit Tags versehen sein](#)
- [\[GuardDuty.3\] GuardDuty IPSets sollte markiert werden](#)
- [\[GuardDuty.4\] GuardDuty Detektoren sollten markiert werden](#)
- [\[IAM.23\] IAM Access Analyzer-Analyzer sollten markiert werden](#)
- [\[IAM.24\] IAM-Rollen sollten mit Tags versehen werden](#)
- [\[IAM.25\] IAM-Benutzer sollten markiert werden](#)
- [\[IoT.1\] AWS IoT Device Defender Sicherheitsprofile sollten markiert werden](#)
- [\[IoT.2\] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden](#)
- [\[IoT.3\] AWS IoT Core -Dimensionen sollten markiert werden](#)
- [\[IoT.4\] AWS IoT Core Autorisierer sollten markiert werden](#)
- [\[IoT.5\] AWS IoT Core Rollenalias sollten markiert werden](#)
- [\[IoT.6\] AWS IoT Core Richtlinien sollten markiert werden](#)
- [\[IoTEvents.1\] AWS IoT-Events-Eingaben sollten markiert werden](#)
- [\[IoTEvents.2\] AWS IoT-Ereignisdetektormodelle sollten markiert werden](#)
- [\[IoTEvents.3\] Alarmmodelle für AWS IoT Events sollten markiert werden](#)
- [\[IoTSiteWise.1\] AWS SiteWise IoT-Asset-Modelle sollten markiert werden](#)
- [\[IoTSiteWise.2\] AWS SiteWise IoT-Dashboards sollten markiert werden](#)
- [\[IoTSiteWise.3\] AWS SiteWise IoT-Gateways sollten markiert werden](#)
- [\[IoTSiteWise.4\] AWS SiteWise IoT-Portale sollten markiert werden](#)
- [\[IoTSiteWise.5\] AWS SiteWise IoT-Projekte sollten markiert werden](#)
- [\[TwinMaker.1\] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden](#)
- [\[TwinMaker.2\] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden](#)

- [\[IoT Twin Maker.3\] AWS TwinMaker IoT-Szenen sollten markiert werden](#)
- [\[IoT Twin Maker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[IoT Wireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[IoT Wireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)
- [\[IoT Wireless .3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)
- [\[Keyspaces.1\] Amazon Keyspaces Keyspaces sollten mit Tags versehen sein](#)
- [\[Kinesis.2\] Kinesis-Streams sollten markiert werden](#)
- [\[Lambda.6\] Lambda-Funktionen sollten markiert werden](#)
- [\[MQ.4\] Amazon MQ-Broker sollten markiert werden](#)
- [\[NetworkFirewall.7\] Netzwerk-Firewall-Firewalls sollten markiert werden](#)
- [\[NetworkFirewall.8\] Firewall-Richtlinien für Netzwerk-Firewalls sollten markiert werden](#)
- [\[Opensearch.9\] OpenSearch -Domains sollten mit Tags versehen werden](#)
- [\[PCA.2\] AWS Private CA-Zertifizierungsstellen sollten gekennzeichnet werden](#)
- [\[RDS.28\] RDS-DB-Cluster sollten markiert werden](#)
- [\[RDS.29\] RDS-DB-Cluster-Snapshots sollten markiert werden](#)
- [\[RDS.30\] RDS-DB-Instances sollten markiert werden](#)
- [\[RDS.31\] RDS-DB-Sicherheitsgruppen sollten markiert werden](#)
- [\[RDS.32\] RDS-DB-Snapshots sollten markiert werden](#)
- [\[RDS.33\] RDS-DB-Subnetzgruppen sollten markiert werden](#)
- [\[Redshift.11\] Redshift-Cluster sollten markiert werden](#)
- [\[Redshift.12\] Abonnements für Redshift-Ereignisbenachrichtigungen sollten markiert werden](#)
- [\[Redshift.13\] Redshift-Cluster-Snapshots sollten markiert werden](#)
- [\[Redshift.14\] Redshift-Cluster-Subnetzgruppen sollten markiert werden](#)
- [\[Redshift.17\] Redshift-Cluster-Parametergruppen sollten markiert werden](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[SageMaker.6\] SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden](#)

- [\[SageMaker.7\] SageMaker Bilder sollten mit Tags versehen werden](#)
- [\[SecretsManager.5\] Secrets Manager Manager-Geheimnisse sollten markiert werden](#)
- [\[SES.1\] SES-Kontaktlisten sollten mit Tags versehen werden](#)
- [\[SES.2\] SES-Konfigurationssätze sollten mit Tags versehen werden](#)
- [\[SNS.3\] SNS-Themen sollten markiert werden](#)
- [\[SQS.2\] SQS-Warteschlangen sollten markiert werden](#)
- [\[SSM.5\] SSM-Dokumente sollten mit Tags versehen werden](#)
- [\[StepFunctions.2\] Die Aktivitäten von Step Functions sollten mit Tags versehen werden](#)
- [\[Transfer.1\] AWS Transfer Family -Workflows sollten mit Tags versehen werden](#)
- [\[Transfer.4\] Transfer Family Familienverträge sollten gekennzeichnet werden](#)
- [\[Transfer.5\] Transfer Family Familienzertifikate sollten gekennzeichnet sein](#)
- [\[Transfer.6\] Steckverbinder der Transfer-Familie sollten gekennzeichnet sein](#)
- [\[Transfer.7\] Familienprofile sollten mit Tags versehen werden](#)

Benchmark der AWS GUS-Stiftungen im Security Hub CSPM

Der Center for Internet Security (CIS) AWS Foundations Benchmark dient als eine Reihe von bewährten Methoden zur Sicherheitskonfiguration für AWS. Diese branchenweit anerkannten Best Practices bieten Ihnen klare step-by-step Implementierungs- und Bewertungsverfahren. Die Kontrollen in diesem Benchmark reichen von Betriebssystemen über Cloud-Dienste bis hin zu Netzwerkgeräten und helfen Ihnen dabei, die spezifischen Systeme zu schützen, die Ihr Unternehmen verwendet.

AWS Security Hub Cloud Security Posture Management (CSPM) unterstützt die Benchmark-Versionen 3.0.0, 1.4.0 und 1.2.0 der CIS AWS Foundations. Auf dieser Seite sind die Sicherheitskontrollen aufgeführt, die jede Version unterstützt. Sie bietet auch einen Vergleich der Versionen.

Benchmark der CIS AWS Foundations Version 3.0.0

Security Hub CSPM unterstützt Version 3.0.0 (v3.0.0) des CIS Foundations Benchmark. AWS Security Hub CSPM hat die Anforderungen der CIS Security Software Certification erfüllt und wurde mit der CIS Security Software Certification für die folgenden CIS-Benchmarks ausgezeichnet:

- CIS Benchmark for CIS AWS Foundations Benchmark, v3.0.0, Stufe 1

- CIS-Benchmark für AWS GUS-Stiftungen, Benchmark, v3.0.0, Stufe 2

Kontrollen, die für CIS AWS Foundations Benchmark Version 3.0.0 gelten

[\[Account.1\] Sicherheitskontaktinformationen sollten bereitgestellt werden für AWS-Konto](#)

[\[CloudTrail.1\] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst](#)

[\[CloudTrail.2\] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben](#)

[\[CloudTrail.4\] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein](#)

[\[CloudTrail.7\] Sicherstellen, dass die S3-Bucket-Zugriffsprotokollierung für den CloudTrail S3-Bucket aktiviert ist](#)

[\[Config.1\] AWS Config sollte aktiviert sein und die serviceverknüpfte Rolle für die Ressourcenaufzeichnung verwenden](#)

[\[EC2.2\] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen](#)

[\[EC2.6\] Die VPC-Flow-Protokollierung sollte in allen aktiviert sein VPCs](#)

[\[EC2.7\] Die EBS-Standardverschlüsselung sollte aktiviert sein](#)

[\[EC2.8\] EC2 Instances sollten Instance Metadata Service Version 2 \(\) verwenden IMDSv2](#)

[\[EC2.21\] Das Netzwerk ACLs sollte keinen Zugang von 0.0.0.0/0 zu Port 22 oder Port 3389 zulassen](#)

[\[EC2.53\] EC2 Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 zu Remote-Serververwaltungsports zulassen](#)

[\[EC2.54\] EC2 Sicherheitsgruppen sollten keinen Zugriff von: :/0 zu Remote-Serveradministrationsports zulassen](#)

[\[EFS.1\] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS](#)

[\[IAM.2\] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein](#)

[\[IAM.3\] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden](#)

[\[IAM.4\] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren](#)

[\[IAM.5\] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen](#)

[\[IAM.6\] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.](#)

[\[IAM.9\] MFA sollte für den Root-Benutzer aktiviert sein](#)

[\[IAM.15\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert](#)

[\[IAM.16\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert](#)

[\[IAM.18\] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS -Support](#)

[\[IAM.22\] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden](#)

[\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)

[\[IAM.27\] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWS Cloud Shell Full Access](#)

[\[IAM.28\] Der externe Zugriffsanalysator für IAM Access Analyzer sollte aktiviert sein](#)

[\[KMS.4\] Die AWS KMS Schlüsselrotation sollte aktiviert sein](#)

[\[RDS.2\] RDS-DB-Instances sollten, wie in der Konfiguration festgelegt, den öffentlichen Zugriff verbieten Publicly Accessible](#)

[\[RDS.3\] Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein.](#)

[\[RDS.13\] Automatische RDS-Upgrades für Nebenversionen sollten aktiviert sein](#)

[\[S3.1\] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein](#)

[\[S3.5\] S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erfordern](#)

[\[S3.8\] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren](#)

[\[S3.20\] Bei S3-Allzweck-Buckets sollte MFA Delete aktiviert sein](#)

[\[S3.22\] S3-Allzweck-Buckets sollten Schreibereignisse auf Objektebene protokollieren](#)

[\[S3.23\] S3-Allzweck-Buckets sollten Leseereignisse auf Objektebene protokollieren](#)

CIS AWS Foundations Benchmark Version 1.4.0

Security Hub CSPM unterstützt Version 1.4.0 (v1.4.0) des CIS Foundations Benchmark. AWS

Kontrollen, die für die Version 1.4.0 von CIS Foundations Benchmark AWS gelten

[\[CloudTrail.1\] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst](#)

[\[CloudTrail.2\] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben](#)

[\[CloudTrail.4\] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein](#)

[\[CloudTrail.5\] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden](#)

[\[CloudTrail.6\] Sicherstellen, dass der S3-Bucket, in dem CloudTrail Protokolle gespeichert werden, nicht öffentlich zugänglich ist](#)

[\[CloudTrail.7\] Sicherstellen, dass die S3-Bucket-Zugriffsprotokollierung für den CloudTrail S3-Bucket aktiviert ist](#)

[\[CloudWatch.1\] Für den Benutzer „root“ sollten ein Filter und ein Alarm für die Log-Metrik vorhanden sein](#)

[\[CloudWatch.4\] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der IAM-Richtlinie vorhanden sind](#)

[\[CloudWatch.5\] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für CloudTrail -Config--Config-Änderungen vorhanden sind](#)

[\[CloudWatch.6\] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für AWS Management Console Authentifizierungsfehler vorhanden sind](#)

[CloudWatch.7] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden verwalteten Schlüsseln vorhanden sind

[CloudWatch.8] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der S3-Bucket-Richtlinie vorhanden sind

[CloudWatch.9] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für AWS Config -Config--Config-Änderungen vorhanden sind

[CloudWatch.10] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Sicherheitsgruppe vorhanden sind

[CloudWatch.11] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind

[CloudWatch.12] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an Network-Gateways vorhanden sind

[CloudWatch.13] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Routing-Tabelle vorhanden sind

[CloudWatch.14] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für VPC-Änderungen vorhanden sind

[Config.1] AWS Config sollte aktiviert sein und die serviceverknüpfte Rolle für die Ressourcenaufzeichnung verwenden

[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen

[EC2.6] Die VPC-Flow-Protokollierung sollte in allen aktiviert sein VPCs

[EC2.7] Die EBS-Standardverschlüsselung sollte aktiviert sein

[EC2.21] Das Netzwerk ACLs sollte keinen Zugang von 0.0.0.0/0 zu Port 22 oder Port 3389 zulassen

[IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen

[IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden

[\[IAM.4\] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren](#)

[\[IAM.5\] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen](#)

[\[IAM.6\] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.](#)

[\[IAM.9\] MFA sollte für den Root-Benutzer aktiviert sein](#)

[\[IAM.15\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert](#)

[\[IAM.16\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert](#)

[\[IAM.18\] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS -Support](#)

[\[IAM.22\] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden](#)

[\[KMS.4\] Die AWS KMS Schlüsselrotation sollte aktiviert sein](#)

[\[RDS.3\] Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein.](#)

[\[S3.1\] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein](#)

[\[S3.5\] S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erfordern](#)

[\[S3.8\] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren](#)

[\[S3.20\] Bei S3-Allzweck-Buckets sollte MFA Delete aktiviert sein](#)

CIS AWS Foundations Benchmark Version 1.2.0

Security Hub CSPM unterstützt Version 1.2.0 (v1.2.0) des CIS Foundations Benchmark. AWS Security Hub CSPM hat die Anforderungen der CIS Security Software Certification erfüllt und wurde mit der CIS Security Software Certification für die folgenden CIS-Benchmarks ausgezeichnet:

- CIS Benchmark for CIS AWS Foundations Benchmark, v1.2.0, Stufe 1
- CIS-Benchmark für AWS GUS-Stiftungen, Benchmark, v1.2.0, Stufe 2

Kontrollen, die für CIS AWS Foundations Benchmark Version 1.2.0 gelten

[CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst

[CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben

[CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein

[CloudTrail.5] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden

[CloudTrail.6] Sicherstellen, dass der S3-Bucket, in dem CloudTrail Protokolle gespeichert werden, nicht öffentlich zugänglich ist

[CloudTrail.7] Sicherstellen, dass die S3-Bucket-Zugriffsprotokollierung für den CloudTrail S3-Bucket aktiviert ist

[CloudWatch.1] Für den Benutzer „root“ sollten ein Filter und ein Alarm für die Log-Metrik vorhanden sein

[CloudWatch.2] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für nicht autorisierte API-Aufrufe vorhanden sind

[CloudWatch.3] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für die Anmeldung in der Managementkonsole ohne MFA vorhanden sind

[CloudWatch.4] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der IAM-Richtlinie vorhanden sind

[CloudWatch.5] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für CloudTrail -Config--Config-Änderungen vorhanden sind

[CloudWatch.6] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für AWS Management Console Authentifizierungsfehler vorhanden sind

[CloudWatch.7] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden verwalteten Schlüsseln vorhanden sind

[CloudWatch.8] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der S3-Bucket-Richtlinie vorhanden sind

[CloudWatch.9] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für AWS Config -Config--Config-Änderungen vorhanden sind

[CloudWatch.10] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Sicherheitsgruppe vorhanden sind

[CloudWatch.11] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind

[CloudWatch.12] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an Network-Gateways vorhanden sind

[CloudWatch.13] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Routing-Tabelle vorhanden sind

[CloudWatch.14] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für VPC-Änderungen vorhanden sind

[Config.1] AWS Config sollte aktiviert sein und die serviceverknüpfte Rolle für die Ressourcenaufzeichnung verwenden

[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen

[EC2.6] Die VPC-Flow-Protokollierung sollte in allen aktiviert sein VPCs

[EC2.13] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen

[EC2.14] Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 oder: :/0 auf Port 3389 zulassen

[IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen

[IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein

[IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden

[IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren

[IAM.5] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen

[IAM.6] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.

[IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden

[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein

[\[IAM.11\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert](#)

[\[IAM.12\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert](#)

[\[IAM.13\] Stellen Sie sicher, dass für die IAM-Passwortrichtlinie mindestens ein Symbol erforderlich ist](#)

[\[IAM.14\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert](#)

[\[IAM.15\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert](#)

[\[IAM.16\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert](#)

[\[IAM.17\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft](#)

[\[IAM.18\] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS -Support](#)

[\[KMS.4\] Die AWS KMS Schlüsselrotation sollte aktiviert sein](#)

Versionsvergleich für CIS AWS Foundations Benchmark

In diesem Abschnitt werden die Unterschiede zwischen bestimmten Versionen des Center for Internet Security (CIS) AWS Foundations Benchmark — v3.0.0, v1.4.0 und v1.2.0 — zusammengefasst. AWS Security Hub Cloud Security Posture Management (CSPM) unterstützt jede dieser Versionen des CIS AWS Foundations Benchmark. Wir empfehlen jedoch, Version 3.0.0 zu verwenden, um über bewährte Sicherheitsmethoden auf dem Laufenden zu bleiben. Sie können mehrere Versionen des Standards gleichzeitig aktivieren. Informationen zur Aktivierung von Standards finden Sie unter [Einen Sicherheitsstandard aktivieren](#). Wenn Sie ein Upgrade auf Version 3.0.0 durchführen möchten, aktivieren Sie es, bevor Sie eine ältere Version deaktivieren. Dadurch werden Lücken in Ihren Sicherheitsüberprüfungen vermieden. [Wenn Sie die Security Hub CSPM-Integration mit verwenden AWS Organizations und v3.0.0 in mehreren Konten stapelweise aktivieren möchten, empfehlen wir die zentrale Konfiguration](#).

Zuordnung der Kontrollen zu den CIS-Anforderungen in jeder Version

Verstehen Sie, welche Kontrollen jede Version des CIS AWS Foundations Benchmark unterstützt.

Kontroll-ID und Titel	Anforderung für CIS v3.0.0	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[Account.1] Sicherheitskontaktinformationen sollten bereitgestellt werden für AWS-Konto	1.2	1.2	1.18
[CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst	3.1	3.1	2.1
[CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben	3.5	3.7	2.7
[CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein	3.2	3.2	2.2
[CloudTrail.5] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden	Nicht unterstützt — CIS hat diese Anforderung entfernt	3.4	2.4
[CloudTrail.6] Sicherstellen, dass der S3-Bucket, in dem CloudTrail Protokolle gespeichert werden, nicht öffentlich zugänglich ist	Nicht unterstützt — CIS hat diese Anforderung entfernt	3.3	2.3
[CloudTrail.7] Sicherstellen, dass die S3-Bucket-Zugriffsprotokollierung für den CloudTrail S3-Bucket aktiviert ist	3.4	3.6	2.6

Kontroll-ID und Titel	Anforderung für CIS v3.0.0	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[CloudWatch.1] Für den Benutzer „root“ sollten ein Filter und ein Alarm für die Log-Metrik vorhanden sein	Nicht unterstützt — manuelle Überprüfung	4.3	3.3
[CloudWatch.2] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für nicht autorisierte API-Aufrufe vorhanden sind	Nicht unterstützt — manuelle Überprüfung	Nicht unterstützt — manuelle Überprüfung	3.1
[CloudWatch.3] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für die Anmeldung in der Managementkonsole ohne MFA vorhanden sind	Nicht unterstützt — manuelle Überprüfung	Nicht unterstützt — manuelle Überprüfung	3.2
[CloudWatch.4] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der IAM-Richtlinie vorhanden sind	Nicht unterstützt — manuelle Überprüfung	4.4	3.4
[CloudWatch.5] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für CloudTrail -Config--Config-Änderungen vorhanden sind	Nicht unterstützt — manuelle Überprüfung	4.5	3.5
[CloudWatch.6] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für AWS Management Console Authentifizierungsfehler vorhanden sind	Nicht unterstützt — manuelle Überprüfung	4.6	3.6

Kontroll-ID und Titel	Anforderung für CIS v3.0.0	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[CloudWatch.7] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden verwalteten Schlüsseln vorhanden sind	Nicht unterstützt — manuelle Überprüfung	4.7	3.7
[CloudWatch.8] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der S3-Bucket-Richtlinie vorhanden sind	Nicht unterstützt — manuelle Überprüfung	4.8	3.8
[CloudWatch.9] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für AWS Config -Config--Config-Änderungen vorhanden sind	Nicht unterstützt — manuelle Überprüfung	4,9 bis 4,9	3.9
[CloudWatch.10] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Sicherheitsgruppe vorhanden sind	Nicht unterstützt — manuelle Überprüfung	4.10	3,10
[CloudWatch.11] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind	Nicht unterstützt — manuelle Überprüfung	4.11	3,11
[CloudWatch.12] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an Network-Gateways vorhanden sind	Nicht unterstützt — manuelle Überprüfung	4.12	3,12

Kontroll-ID und Titel	Anforderung für CIS v3.0.0	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[CloudWatch.13] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Routing-Tabelle vorhanden sind	Nicht unterstützt — manuelle Überprüfung	4.13	3.13
[CloudWatch.14] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für VPC-Änderungen vorhanden sind	Nicht unterstützt — manuelle Überprüfung	4.14	3,14
[Config.1] AWS Config sollte aktiviert sein und die serviceverknüpfte Rolle für die Ressourcenaufzeichnung verwenden	3.3	3.5	2.5
[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen	5.4	5.3	4.3
[EC2.6] Die VPC-Flow-Protokollierung sollte in allen aktiviert sein VPCs	3.7	3.9	2,9
[EC2.7] Die EBS-Standardverschlüsselung sollte aktiviert sein	2.2.1	2.2.1	Nicht unterstützt
[EC2.8] EC2 Instances sollten Instance Metadata Service Version 2 () verwenden IMDSv2	5.6	Nicht unterstützt	Nicht unterstützt
[EC2.13] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen	Nicht unterstützt — ersetzt durch die Anforderungen 5.2 und 5.3	Nicht unterstützt — ersetzt durch die Anforderungen 5.2 und 5.3	4.1

Kontroll-ID und Titel	Anforderung für CIS v3.0.0	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[EC2.14] Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 oder: :/0 auf Port 3389 zulassen	Nicht unterstützt — ersetzt durch die Anforderungen 5.2 und 5.3	Nicht unterstützt — ersetzt durch die Anforderungen 5.2 und 5.3	4.2
[EC2.21] Das Netzwerk ACLs sollte keinen Zugang von 0.0.0.0/0 zu Port 22 oder Port 3389 zulassen	5.1	5.1	Nicht unterstützt
[EC2.53] EC2 Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 zu Remote-Serververwaltungsports zulassen	5.2	Nicht unterstützt	Nicht unterstützt
[EC2.54] EC2 Sicherheitsgruppen sollten keinen Zugriff von: :/0 zu Remote-Serveradministrationsports zulassen	5.3	Nicht unterstützt	Nicht unterstützt
[EFS.1] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS	2.4.1	Nicht unterstützt	Nicht unterstützt
[IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen	Nicht unterstützt	1.16	1,22
[IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein	1.15	Nicht unterstützt	1.16
[IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden	1.14	1.14	1.4

Kontroll-ID und Titel	Anforderung für CIS v3.0.0	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren	1.4	1.4	1.12
[IAM.5] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen	1.10	1.10	1.2
[IAM.6] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.	1,6	1,6	1.14
[IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden	Wird nicht unterstützt — siehe stattdessen [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden	Nicht unterstützt — siehe [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden stattdessen	1.3
[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein	1.5	1.5	1.13
[IAM.11] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert	Nicht unterstützt — CIS hat diese Anforderung entfernt	Nicht unterstützt — CIS hat diese Anforderung entfernt	1.5
[IAM.12] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert	Nicht unterstützt — CIS hat diese Anforderung entfernt	Nicht unterstützt — CIS hat diese Anforderung entfernt	1,6

Kontroll-ID und Titel	Anforderung für CIS v3.0.0	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[IAM.13] Stellen Sie sicher, dass für die IAM-Passwortrichtlinie mindestens ein Symbol erforderlich ist	Nicht unterstützt — CIS hat diese Anforderung entfernt	Nicht unterstützt — CIS hat diese Anforderung entfernt	1,7
[IAM.14] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert	Nicht unterstützt — CIS hat diese Anforderung entfernt	Nicht unterstützt — CIS hat diese Anforderung entfernt	1.8
[IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert	1.8	1.8	1.9
[IAM.16] Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert	1.9	1.9	1.10
[IAM.17] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft	Nicht unterstützt — CIS hat diese Anforderung entfernt	Nicht unterstützt — CIS hat diese Anforderung entfernt	1.11
[IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS - Support	1,17	1,17	1.2
[IAM.20] Vermeiden Sie die Verwendung des Root-Benutzers	Nicht unterstützt — CIS hat diese Anforderung entfernt	Nicht unterstützt — CIS hat diese Anforderung entfernt	1.1

Kontroll-ID und Titel	Anforderung für CIS v3.0.0	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden	1.12	1.12	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt
[IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden	1.19	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt
[IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein <u>AWSCloud ShellFullAccess</u>	1.22	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt
[IAM.28] Der externe Zugriffsanalysator für IAM Access Analyzer sollte aktiviert sein	1.20	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt
[KMS.4] Die AWS KMS Schlüsselrotation sollte aktiviert sein	3.6	3.8	2.8
[Macie.1] Amazon Macie sollte aktiviert sein	Nicht unterstützt — manuelle Überprüfung	Nicht unterstützt — manuelle Überprüfung	Nicht unterstützt — manuelle Überprüfung

Kontroll-ID und Titel	Anforderung für CIS v3.0.0	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[RDS.2] RDS-DB-Instances sollten, wie in der Konfiguration festgelegt, den öffentlichen Zugriff verbieten PubliclyAccessible	2.3.3	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt
[RDS.3] Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein.	2.3.1	2.3.1	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt
[RDS.13] Automatische RDS-Upgrades für Nebenversionen sollten aktiviert sein	2.3.2	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt
[S3.1] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein	2.1.4	2.1.5	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt
[S3.5] S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erfordern	2.1.1	2.1.2	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt

Kontroll-ID und Titel	Anforderung für CIS v3.0.0	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren	2.1.4	2.1.5	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt
[S3.20] Bei S3-Allzweck-Buckets sollte MFA Delete aktiviert sein	2.1.2	2.1.3	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt

ARNs für Benchmarks der CIS AWS Foundations

Wenn Sie eine oder mehrere Versionen von CIS AWS Foundations Benchmark aktivieren, erhalten Sie die Ergebnisse ab sofort im AWS Security Finding Format (ASFF). In ASFF verwendet jede Version den folgenden Amazon-Ressourcennamen (ARN):

Benchmark AWS v3.0.0 für CIS Foundations

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/v/3.0.0
```

Benchmark v1.4.0 für AWS GUS-Stiftungen

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/v/1.4.0
```

Benchmark v1.2.0 AWS für GUS-Stiftungen

```
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0
```

Sie können den [GetEnabledStandards](#) Betrieb der Security Hub CSPM-API verwenden, um den ARN eines aktivierten Standards zu ermitteln.

Die vorherigen Werte sind für `StandardsArn` `StandardsSubscriptionArn`Bezieht sich jedoch auf die Standard-Abonnementressource, die Security Hub CSPM erstellt, wenn Sie einen Standard abonnieren, indem Sie [BatchEnableStandards](#) in einer Region anrufen.

 Note

Wenn Sie eine Version des CIS AWS Foundations Benchmark aktivieren, kann es bis zu 18 Stunden dauern, bis Security Hub CSPM Ergebnisse für Kontrollen generiert, die dieselbe AWS Config serviceverknüpfte Regel verwenden wie aktivierte Kontrollen in anderen aktivierten Standards. Weitere Informationen zum Zeitplan für die Generierung von Kontrollbefunden finden Sie unter [Zeitplan für die Ausführung von Sicherheitsprüfungen](#)

Suchfelder unterscheiden sich, wenn Sie konsolidierte Kontrollergebnisse aktivieren. Informationen zu diesen Unterschieden finden Sie unter [Auswirkungen der Konsolidierung auf ASFF-Felder und -Werte](#). Ergebnisse der Stichprobenkontrolle finden Sie unter [Stichproben von Kontrollbefunden](#).

CIS-Anforderungen, die in Security Hub CSPM nicht unterstützt werden

Wie in der obigen Tabelle erwähnt, unterstützt Security Hub CSPM nicht jede CIS-Anforderung in jeder Version des CIS AWS Foundations Benchmark. Viele der nicht unterstützten Anforderungen können nur bewertet werden, indem der Status Ihrer Ressourcen manuell überprüft wird. AWS

NIST SP 800-53 Revision 5 im Security Hub CSPM

Die NIST-Sonderveröffentlichung 800-53 Revision 5 (NIST SP 800-53 Rev. 5) ist ein Framework für Cybersicherheit und Compliance, das vom National Institute of Standards and Technology (NIST), einer Behörde, die Teil des US-Handelsministeriums ist, entwickelt wurde. Dieses Compliance-Framework enthält einen Katalog von Sicherheits- und Datenschutzerfordernungen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationssystemen und kritischen Ressourcen. US-Bundesbehörden und Auftragnehmer müssen diese Anforderungen erfüllen, um ihre Systeme und Organisationen zu schützen. Private Organisationen können die Anforderungen auch freiwillig als Leitfaden für die Reduzierung des Cybersicherheitsrisikos verwenden. Weitere Informationen zum Framework und seinen Anforderungen finden Sie unter [NIST SP 800-53 Rev. 5](#) im NIST Computer Security Resource Center.

AWS Security Hub Cloud Security Posture Management (CSPM) bietet Sicherheitskontrollen, die einen Teil der Anforderungen von NIST SP 800-53 Revision 5 unterstützen. Die Kontrollen

führen automatisierte Sicherheitsprüfungen für bestimmte Ressourcen durch. AWS-Services Um diese Kontrollen zu aktivieren und zu verwalten, können Sie das NIST SP 800-53 Revision 5-Framework standardmäßig in Security Hub CSPM aktivieren. Beachten Sie, dass die Steuerungen die Anforderungen von NIST SP 800-53 Revision 5, die manuelle Prüfungen erfordern, nicht unterstützen.

Im Gegensatz zu anderen Frameworks schreibt das NIST SP 800-53 Revision 5-Framework nicht vor, wie seine Anforderungen bewertet werden sollten. Stattdessen enthält das Framework Richtlinien. In Security Hub CSPM stellen der Standard und die Kontrollen von NIST SP 800-53 Revision 5 das Verständnis des Dienstes in Bezug auf diese Richtlinien dar.

Themen

- [Konfiguration der Ressourcenaufzeichnung für Kontrollen, die für den Standard gelten](#)
- [Feststellen, welche Kontrollen für den Standard gelten](#)

Konfiguration der Ressourcenaufzeichnung für Kontrollen, die für den Standard gelten

Um die Abdeckung und die Genauigkeit der Ergebnisse zu optimieren, ist es wichtig, die Ressourcenaufzeichnung zu aktivieren und zu konfigurieren, AWS Config bevor Sie den Standard NIST SP 800-53 Revision 5 in AWS Security Hub Cloud Security Posture Management (CSPM) aktivieren. Achten Sie bei der Konfiguration der Ressourcenaufzeichnung auch darauf, sie für alle AWS Ressourcentypen zu aktivieren, die durch die für den Standard geltenden Kontrollen überprüft werden. Dies gilt in erster Linie für Steuerelemente mit einem Zeitplantyp, der durch Änderung ausgelöst wurde. Für einige Steuerelemente mit einem periodischen Zeitplan ist jedoch auch die Erfassung von Ressourcen erforderlich. Wenn die Ressourcenaufzeichnung nicht aktiviert oder korrekt konfiguriert ist, ist Security Hub CSPM möglicherweise nicht in der Lage, die entsprechenden Ressourcen zu bewerten und genaue Ergebnisse für Kontrollen zu generieren, die für den Standard gelten.

Informationen darüber, wie Security Hub CSPM die Ressourcenaufzeichnung in verwendet AWS Config, finden Sie unter [Aktivierung und Konfiguration AWS Config für Security Hub CSPM](#). Informationen zur Konfiguration der Ressourcenaufzeichnung in AWS Config finden Sie unter [Arbeiten mit dem Konfigurationsrekorder](#) im AWS Config Entwicklerhandbuch.

In der folgenden Tabelle sind die Ressourcentypen aufgeführt, die für Kontrollen aufgezeichnet werden müssen, die für den Standard NIST SP 800-53 Revision 5 in Security Hub CSPM gelten.

AWS-Service	Ressourcentypen
Amazon API Gateway	AWS::ApiGateway::Stage , AWS::ApiGatewayV2::Stage
AWS AppSync	AWS::AppSync::GraphQLApi
AWS Backup	AWS::Backup::RecoveryPoint
AWS Certificate Manager (ACM)	AWS::ACM::Certificate
AWS CloudFormation	AWS::CloudFormation::Stack
Amazon CloudFront	AWS::CloudFront::Distribution
Amazon CloudWatch	AWS::CloudWatch::Alarm
AWS CodeBuild	AWS::CodeBuild::Project
AWS Database Migration Service (AWS DMS)	AWS::DMS::Endpoint , AWS::DMS::ReplicationInstance , AWS::DMS::ReplicationTask
Amazon-DynamoDB	AWS::DynamoDB::Table
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::ClientVpnEndpoint , AWS::EC2::EIP , AWS::EC2::Instance , AWS::EC2::LaunchTemplate , AWS::EC2::NetworkAcl , AWS::EC2::NetworkInterface , AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::TransitGateway , AWS::EC2::VPNConnection , AWS::EC2::Volume
Amazon EC2 Auto Scaling	AWS::AutoScaling::AutoScalingGroup , AWS::AutoScaling::LaunchConfiguration

AWS-Service	Ressourcentypen
Amazon Elastic Container Registry (Amazon ECR)	<code>AWS::ECR::Repository</code>
Amazon Elastic Container Service (Amazon ECS)	<code>AWS::ECS::Cluster</code> , <code>AWS::ECS::Service</code> , <code>AWS::ECS::TaskDefinition</code>
Amazon Elastic File System (Amazon EFS)	<code>AWS::EFS::AccessPoint</code>
Amazon Elastic Kubernetes Service (Amazon EKS)	<code>AWS::EKS::Cluster</code>
AWS Elastic Beanstalk	<code>AWS::ElasticBeanstalk::Environment</code>
Elastic Load Balancing	<code>AWS::ElasticLoadBalancing::LoadBalancer</code> , <code>AWS::ElasticLoadBalancingV2::Listener</code> , <code>AWS::ElasticLoadBalancingV2::LoadBalancer</code>
Amazon ElasticSearch	<code>AWS::Elasticsearch::Domain</code>
Amazon EMR	<code>AWS::EMR::SecurityConfiguration</code>
Amazon EventBridge	<code>AWS::Events::Endpoint</code> , <code>AWS::Events::EventBus</code>
AWS Glue	<code>AWS::Glue::Job</code>
AWS Identity and Access Management (IAM)	<code>AWS::IAM::Group</code> , <code>AWS::IAM::Policy</code> , <code>AWS::IAM::Role</code> , <code>AWS::IAM::User</code>
AWS Key Management Service (AWS KMS)	<code>AWS::KMS::Alias</code> , <code>AWS::KMS::Key</code>
Amazon Kinesis	<code>AWS::Kinesis::Stream</code>
AWS Lambda	<code>AWS::Lambda::Function</code>

AWS-Service	Ressourcentypen
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	<code>AWS::MSK::Cluster</code>
Amazon MQ	<code>AWS::AmazonMQ::Broker</code>
AWS Network Firewall	<code>AWS::NetworkFirewall::Firewall</code> , <code>AWS::NetworkFirewall::FirewallPolicy</code> , <code>AWS::NetworkFirewall::RuleGroup</code>
OpenSearch Amazon-Dienst	<code>AWS::OpenSearch::Domain</code>
Amazon Relational Database Service (Amazon RDS)	<code>AWS::RDS::DBCluster</code> , <code>AWS::RDS::DBClusterSnapshot</code> , <code>AWS::RDS::DBInstance</code> , <code>AWS::RDS::DBSnapshot</code> , <code>AWS::RDS::EventSubscription</code>
Amazon Redshift	<code>AWS::Redshift::Cluster</code> , <code>AWS::Redshift::ClusterSubnetGroup</code>
Amazon Route 53	<code>AWS::Route53::HostedZone</code>
Amazon Simple Storage Service (Amazon-S3)	<code>AWS::S3::AccessPoint</code> , <code>AWS::S3::AccountPublicAccessBlock</code> , <code>AWS::S3::Bucket</code>
AWS Service Catalog	<code>AWS::ServiceCatalog::Portfolio</code>
Amazon-Simple-Notification-Service (Amazon-SNS)	<code>AWS::SNS::Topic</code>
Amazon-Simple-Queue-Service (Amazon SQS)	<code>AWS::SQS::Queue</code>
EC2 Amazon-Systemmanager (SSM)	<code>AWS::SSM::AssociationCompliance</code> , <code>AWS::SSM::ManagedInstanceInventory</code> , <code>AWS::SSM::PatchCompliance</code>

AWS-Service	Ressourcentypen
Amazon SageMaker KI	AWS::SageMaker::NotebookInstance
AWS Secrets Manager	AWS::SecretsManager::Secret
AWS Transfer Family	AWS::Transfer::Connector
AWS WAF	AWS::WAF::Rule , AWS::WAF::RuleGroup , AWS::WAF::WebACL , AWS::WAFRegional::Rule , AWS::WAFRegional::RuleGroup , AWS::WAFRegional::WebACL , AWS::WAFv2::RuleGroup , AWS::WAFv2::WebACL

Feststellen, welche Kontrollen für den Standard gelten

In der folgenden Liste sind die Kontrollen aufgeführt, die die Anforderungen von NIST SP 800-53 Revision 5 unterstützen und für den Standard NIST SP 800-53 Revision 5 in AWS Security Hub Cloud Security Posture Management (CSPM) gelten. Einzelheiten zu den spezifischen Anforderungen, die ein Steuerelement unterstützt, erhalten Sie, wenn Sie das Steuerelement auswählen. Weitere Informationen finden Sie in den Details für das Steuerelement im Feld „Verwandte Anforderungen“. Dieses Feld gibt jede NIST-Anforderung an, die das Steuerelement unterstützt. Wenn das Feld keine bestimmte NIST-Anforderung spezifiziert, unterstützt das Steuerelement die Anforderung nicht.

- [\[Account.1\] Sicherheitskontaktinformationen sollten bereitgestellt werden für AWS-Konto](#)
- [\[Account.2\] AWS-Konten sollte Teil einer Organisation sein AWS Organizations](#)
- [\[ACM.1\] Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden](#)
- [\[APIGateway.1\] API Gateway REST und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein](#)
- [\[APIGateway.2\] API Gateway REST API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden](#)
- [\[APIGateway.3\] Bei den REST-API-Stufen von API Gateway sollte die AWS X-Ray Ablaufverfolgung aktiviert sein](#)

- [\[APIGateway.4\] API Gateway sollte mit einer WAF-Web-ACL verknüpft sein](#)
- [\[APIGateway.5\] API Gateway REST API-Cache-Daten sollten im Ruhezustand verschlüsselt werden](#)
- [\[APIGateway.8\] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben](#)
- [\[APIGateway.9\] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein](#)
- [\[AppSync.5\] AWS AppSync GraphQL APIs sollte nicht mit API-Schlüsseln authentifiziert werden](#)
- [\[AutoScaling.1\] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden](#)
- [\[AutoScaling.2\] Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken](#)
- [\[AutoScaling.3\] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2 Instances so konfigurieren, dass sie Instance Metadata Service Version 2 \(IMDSv2\) benötigen](#)
- [\[Autoscaling.5\] EC2 Amazon-Instances, die mit Auto Scaling Scaling-Gruppenstartkonfigurationen gestartet wurden, sollten keine öffentlichen IP-Adressen haben](#)
- [\[AutoScaling.6\] Auto Scaling Scaling-Gruppen sollten mehrere Instance-Typen in mehreren Availability Zones verwenden](#)
- [\[AutoScaling.9\] Amazon EC2 Auto Scaling Scaling-Gruppen sollten EC2 Amazon-Startvorlagen verwenden](#)
- [\[Backup.1\] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)

- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudTrail.1\] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst](#)
- [\[CloudTrail.2\] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben](#)
- [\[CloudTrail.4\] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein](#)
- [\[CloudTrail.5\] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden](#)
- [\[CloudTrail.10\] Event-Datenspeicher in CloudTrail Lake sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys](#)
- [\[CloudWatch.15\] Für CloudWatch Alarmer sollten bestimmte Aktionen konfiguriert sein](#)
- [\[CloudWatch.16\] CloudWatch Protokollgruppen sollten für einen bestimmten Zeitraum aufbewahrt werden](#)
- [\[CloudWatch.17\] CloudWatch Alarmaktionen sollten aktiviert sein](#)
- [\[CodeBuild.1\] Das CodeBuild Bitbucket-Quell-Repository URLs sollte keine vertraulichen Anmeldeinformationen enthalten](#)
- [\[CodeBuild.2\] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten](#)
- [\[CodeBuild.3\] CodeBuild S3-Protokolle sollten verschlüsselt sein](#)
- [\[CodeBuild.4\] CodeBuild Projektumgebungen sollten eine AWS Config Protokollierungsdauer haben](#)
- [\[Config.1\] AWS Config sollte aktiviert sein und die serviceverknüpfte Rolle für die Ressourcenaufzeichnung verwenden](#)
- [\[DataFirehose.1\] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden](#)
- [\[DMS.1\] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein](#)
- [\[DMS.6\] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein](#)
- [\[DMS.7\] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.8\] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.9\] DMS-Endpunkte sollten SSL verwenden](#)

- [\[DMS.10\] Bei DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein](#)
- [\[DMS.11\] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein](#)
- [\[DMS.12\] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein](#)
- [\[DocumentDB.1\] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DocumentDB.2\] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen](#)
- [\[DocumentDB.3\] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein](#)
- [\[DocumentDB.4\] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch](#)
- [\[DocumentDB.5\] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[DynamoDB.1\] DynamoDB-Tabellen sollten die Kapazität automatisch bei Bedarf skalieren](#)
- [\[DynamoDB.2\] Bei DynamoDB-Tabellen sollte die Wiederherstellung aktiviert sein point-in-time](#)
- [\[DynamoDB.3\] DynamoDB Accelerator \(DAX\) -Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DynamoDB.4\] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein](#)
- [\[DynamoDB.6\] Bei DynamoDB-Tabellen sollte der Löschschutz aktiviert sein](#)
- [\[DynamoDB.7\] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[EC2.1\] Amazon EBS-Snapshots sollten nicht öffentlich wiederherstellbar sein](#)
- [\[EC2.2\] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen](#)
- [\[EC2.3\] Angehängte Amazon EBS-Volumes sollten im Ruhezustand verschlüsselt werden](#)
- [\[EC2.4\] Gestoppte EC2 Instances sollten nach einem bestimmten Zeitraum entfernt werden](#)
- [\[EC2.6\] Die VPC-Flow-Protokollierung sollte in allen aktiviert sein VPCs](#)
- [\[EC2.7\] Die EBS-Standardverschlüsselung sollte aktiviert sein](#)
- [\[EC2.8\] EC2 Instances sollten Instance Metadata Service Version 2 \(\) verwenden IMDSv2](#)
- [\[EC2.9\] EC2 Amazon-Instances sollten keine öffentliche IPv4 Adresse haben](#)
- [\[EC2.10\] Amazon EC2 sollte so konfiguriert sein, dass es VPC-Endpunkte verwendet, die für den Amazon-Service erstellt wurden EC2](#)

- [\[EC2.12\] Unbenutztes Amazon EC2 EIPs sollte entfernt werden](#)
- [\[EC2.13\] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder :/0 zu Port 22 zulassen](#)
- [\[EC2.15\] EC2 Amazon-Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen](#)
- [\[EC2.16\] Ungenutzte Network Access Control Lists sollten entfernt werden](#)
- [\[EC2.17\] EC2 Amazon-Instances sollten nicht mehrere verwenden ENIs](#)
- [\[EC2.18\] Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Datenverkehr für autorisierte Ports zulassen](#)
- [\[EC2.19\] Sicherheitsgruppen sollten keinen uneingeschränkten Zugriff auf Ports mit hohem Risiko zulassen](#)
- [\[EC2.20\] Beide VPN-Tunnel für eine AWS Site-to-Site VPN-Verbindung sollten aktiv sein](#)
- [\[EC2.21\] Das Netzwerk ACLs sollte keinen Zugang von 0.0.0.0/0 zu Port 22 oder Port 3389 zulassen](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways sollte VPC-Anhangsanfragen nicht automatisch akzeptieren](#)
- [\[EC2.24\] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden](#)
- [\[EC2.25\] EC2 Amazon-Startvorlagen sollten Netzwerkschnittstellen nicht öffentlich IPs zuweisen](#)
- [\[EC2.28\] EBS-Volumes sollten durch einen Backup-Plan abgedeckt sein](#)
- [\[EC2.51\] EC2 Client-VPN-Endpunkte sollten die Client-Verbindungsprotokollierung aktiviert haben](#)
- [\[EC2.55\] VPCs sollte mit einem Schnittstellenendpunkt für die ECR-API konfiguriert werden](#)
- [\[EC2.56\] VPCs sollte mit einem Schnittstellenendpunkt für Docker Registry konfiguriert werden](#)
- [\[EC2.57\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager konfiguriert werden](#)
- [\[EC2.58\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert sein](#)
- [\[EC2.60\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden](#)
- [\[ECR.1\] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein](#)
- [\[ECR.2\] Bei privaten ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein](#)
- [\[ECR.3\] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein](#)
- [\[ECR.5\] ECR-Repositorys sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys](#)
- [\[ECS.1\] Amazon ECS-Aufgabendefinitionen sollten sichere Netzwerkmodi und Benutzerdefinitionen enthalten](#)

- [\[ECS.2\] ECS-Diensten sollten nicht automatisch öffentliche IP-Adressen zugewiesen werden](#)
- [\[ECS.3\] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen](#)
- [\[ECS.4\] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden](#)
- [\[ECS.5\] ECS-Container sollten auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sein](#)
- [\[ECS.8\] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden](#)
- [\[ECS.9\] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen](#)
- [\[ECS.10\] Die ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen](#)
- [\[ECS.12\] ECS-Cluster sollten Container Insights verwenden](#)
- [\[ECS.17\] ECS-Aufgabendefinitionen sollten nicht den Host-Netzwerkmodus verwenden](#)
- [\[EFS.1\] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS](#)
- [\[EFS.2\] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein](#)
- [\[EFS.3\] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen](#)
- [\[EFS.4\] EFS-Zugangspunkte sollten eine Benutzeridentität erzwingen](#)
- [\[EFS.6\] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden](#)
- [\[EKS.1\] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein](#)
- [\[EKS.2\] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden](#)
- [\[EKS.3\] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden](#)
- [\[EKS.8\] Bei EKS-Clustern sollte die Auditprotokollierung aktiviert sein](#)
- [Bei \[ElastiCache.1\] ElastiCache \(Redis OSS\) -Clustern sollten automatische Backups aktiviert sein](#)
- [\[ElastiCache.2\] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein](#)
- [\[ElastiCache.3\] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein](#)
- [\[ElastiCache.4\] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden](#)
- [\[ElastiCache.5\] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden](#)
- [\[ElastiCache.6\] Für Replikationsgruppen ElastiCache \(Redis OSS\) früherer Versionen sollte Redis OSS AUTH aktiviert sein](#)
- [\[ElastiCache.7\] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden](#)

- [\[ElasticBeanstalk.1\] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben](#)
- [\[ElasticBeanstalk.2\] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein](#)
- [\[ELB.1\] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden](#)
- [\[ELB.2\] Classic Load Balancer mit SSL/HTTPS Listnern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager](#)
- [\[ELB.3\] Classic Load Balancer Balancer-Listener sollten mit HTTPS- oder TLS-Terminierung konfiguriert werden](#)
- [\[ELB.4\] Application Load Balancer sollte so konfiguriert sein, dass ungültige HTTP-Header gelöscht werden](#)
- [\[ELB.5\] Die Protokollierung von Anwendungen und Classic Load Balancers sollte aktiviert sein](#)
- [\[ELB.6\] Für Anwendungen, Gateways und Network Load Balancers sollte der Löschschutz aktiviert sein](#)
- [\[ELB.7\] Bei Classic Load Balancers sollte der Verbindungsabbau aktiviert sein](#)
- [\[ELB.8\] Classic Load Balancer mit SSL-Listnern sollten eine vordefinierte Sicherheitsrichtlinie mit starker Dauer verwenden AWS Config](#)
- [\[ELB.9\] Bei Classic Load Balancers sollte der zonenübergreifende Load Balancing aktiviert sein](#)
- [\[ELB.10\] Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken](#)
- [\[ELB.12\] Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden](#)
- [\[ELB.13\] Anwendungs-, Netzwerk- und Gateway-Load Balancer sollten sich über mehrere Availability Zones erstrecken](#)
- [\[ELB.14\] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden](#)
- [\[ELB.16\] Application Load Balancers sollten mit einer Web-ACL verknüpft sein AWS WAF](#)
- [\[ELB.17\] Anwendungs- und Netzwerk-Load-Balancer mit Listnern sollten die empfohlenen Sicherheitsrichtlinien verwenden](#)
- [\[EMR.1\] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben](#)
- [\[EMR.2\] Die Amazon EMR-Einstellung zum Blockieren des öffentlichen Zugriffs sollte aktiviert sein](#)
- [\[EMR.3\] Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden](#)

- [\[EMR.4\] Amazon EMR-Sicherheitskonfigurationen sollten bei der Übertragung verschlüsselt werden](#)
- [\[ES.1\] Bei Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein](#)
- [\[ES.2\] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein](#)
- [\[ES.3\] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden](#)
- [\[ES.4\] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein](#)
- [\[ES.5\] Für Elasticsearch-Domains sollte die Audit-Protokollierung aktiviert sein](#)
- [\[ES.6\] Elasticsearch-Domains sollten mindestens drei Datenknoten haben](#)
- [\[ES.7\] Elasticsearch-Domänen sollten mit mindestens drei dedizierten Master-Knoten konfiguriert werden](#)
- [\[ES.8\] Verbindungen zu Elasticsearch-Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden](#)
- [\[EventBridge.3\] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden](#)
- [\[EventBridge.4\] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein](#)
- [\[FSx.1\] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden](#)
- [\[FSx.2\] FSx für Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden](#)
- [\[Glue.4\] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue](#)
- [\[GuardDuty.1\] GuardDuty sollte aktiviert sein](#)
- [\[IAM.1\] IAM-Richtlinien sollten keine vollen „*“-Administratorrechte zulassen](#)
- [\[IAM.2\] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein](#)
- [\[IAM.3\] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden](#)
- [\[IAM.4\] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren](#)
- [\[IAM.5\] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen](#)
- [\[IAM.6\] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.](#)
- [\[IAM.7\] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein](#)
- [\[IAM.8\] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden](#)

- [\[IAM.9\] MFA sollte für den Root-Benutzer aktiviert sein](#)
- [\[IAM.19\] MFA sollte für alle IAM-Benutzer aktiviert sein](#)
- [\[IAM.21\] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen](#)
- [\[Kinesis.1\] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden](#)
- [\[KMS.1\] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)
- [\[KMS.2\] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)
- [\[KMS.3\] AWS KMS keys sollte nicht unbeabsichtigt gelöscht werden](#)
- [\[KMS.4\] Die AWS KMS Schlüsselrotation sollte aktiviert sein](#)
- [\[Lambda.1\] Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten](#)
- [\[Lambda.2\] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden](#)
- [\[Lambda.3\] Lambda-Funktionen sollten sich in einer VPC befinden](#)
- [\[Lambda.5\] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren](#)
- [\[Lambda.7\] Bei Lambda-Funktionen sollte aktives Tracing aktiviert sein AWS X-Ray](#)
- [\[Macie.1\] Amazon Macie sollte aktiviert sein](#)
- [\[Macie.2\] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein](#)
- [\[MSK.1\] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden](#)
- [\[MSK.2\] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein](#)
- [\[MQ.2\] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch](#)
- [\[MQ.3\] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein](#)
- [\[MQ.5\] ActiveMQ-Broker sollten den Aktiv-/Standby-Bereitstellungsmodus verwenden](#)
- [\[MQ.6\] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden](#)
- [\[Neptune.1\] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.2\] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)
- [\[Neptune.3\] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein](#)
- [\[Neptune.4\] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[Neptune.5\] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein](#)
- [\[Neptune.6\] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden](#)

- [\[Neptune.7\] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein](#)
- [\[Neptune.8\] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren](#)
- [\[Neptune.9\] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden](#)
- [\[NetworkFirewall.1\] Network firewalls sollten über mehrere Availability Zones hinweg bereitgestellt werden](#)
- [\[NetworkFirewall.2\] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein](#)
- [\[NetworkFirewall.3\] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet haben](#)
- [\[NetworkFirewall.4\] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ sein.](#)
- [\[NetworkFirewall.5\] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ sein.](#)
- [\[NetworkFirewall.6\] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein](#)
- [\[NetworkFirewall.9\] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein](#)
- [\[NetworkFirewall.10\] Bei Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein](#)
- [Bei \[Opensearch.1\] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein](#)
- [\[Opensearch.2\] OpenSearch -Domains sollten nicht öffentlich zugänglich sein](#)
- [\[Opensearch.3\] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden](#)
- [Die Protokollierung von \[Opensearch.4\] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein](#)
- [Für \[Opensearch.5\] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein](#)
- [\[Opensearch.6\] OpenSearch Domains sollten mindestens drei Datenknoten haben](#)
- [Für \[Opensearch.7\] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein](#)
- [\[Opensearch.8\] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden](#)
- [Auf \[Opensearch.10\] OpenSearch -Domains sollte das neueste Softwareupdate installiert sein](#)
- [\[Opensearch.11\] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben](#)
- [\[PCA.1\] AWS Private CA Root-Zertifizierungsstelle sollte deaktiviert sein](#)

- [\[RDS.1\] Der RDS-Snapshot sollte privat sein](#)
- [\[RDS.2\] RDS-DB-Instances sollten, wie in der Konfiguration festgelegt, den öffentlichen Zugriff verbieten PubliclyAccessible](#)
- [\[RDS.3\] Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein.](#)
- [\[RDS.4\] RDS-Cluster-Snapshots und Datenbank-Snapshots sollten im Ruhezustand verschlüsselt werden](#)
- [\[RDS.5\] RDS-DB-Instances sollten mit mehreren Availability Zones konfiguriert werden](#)
- [\[RDS.6\] Die erweiterte Überwachung sollte für RDS-DB-Instances konfiguriert werden](#)
- [\[RDS.7\] Bei RDS-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[RDS.8\] Für RDS-DB-Instances sollte der Löschschutz aktiviert sein](#)
- [\[RDS.9\] RDS-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[RDS.10\] Die IAM-Authentifizierung sollte für RDS-Instances konfiguriert werden](#)
- [\[RDS.11\] Bei RDS-Instances sollten automatische Backups aktiviert sein](#)
- [\[RDS.12\] Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden](#)
- [\[RDS.13\] Automatische RDS-Upgrades für Nebenversionen sollten aktiviert sein](#)
- [\[RDS.14\] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein](#)
- [\[RDS.15\] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden](#)
- [\[RDS.16\] Aurora-DB-Cluster sollten so konfiguriert sein, dass sie Tags in DB-Snapshots kopieren](#)
- [\[RDS.17\] RDS-DB-Instances sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren](#)
- [\[RDS.19\] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Cluster-Ereignisse konfiguriert werden](#)
- [\[RDS.20\] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Ereignisse der Datenbankinstanz konfiguriert werden](#)
- [\[RDS.21\] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbankparametergruppenereignisse konfiguriert werden](#)
- [\[RDS.22\] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbanksicherheitsgruppenereignisse konfiguriert werden](#)
- [\[RDS.23\] RDS-Instances sollten keinen Standard-Port für die Datenbank-Engine verwenden](#)
- [\[RDS.24\] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden](#)

- [\[RDS.25\] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden](#)
- [\[RDS.26\] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden](#)
- [\[RDS.27\] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[RDS.34\] Aurora MySQL-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)
- [\[RDS.35\] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein](#)
- [\[RDS.40\] RDS für SQL Server-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[RDS.42\] RDS für MariaDB-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[RDS.45\] Bei Aurora MySQL-DB-Clustern sollte die Audit-Protokollierung aktiviert sein](#)
- [\[Redshift.1\] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten](#)
- [\[Redshift.2\] Verbindungen zu Amazon Redshift Redshift-Clustern sollten bei der Übertragung verschlüsselt werden](#)
- [\[Redshift.3\] Bei Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein](#)
- [\[Redshift.4\] Bei Amazon Redshift Redshift-Clustern sollte die Auditprotokollierung aktiviert sein](#)
- [\[Redshift.6\] Bei Amazon Redshift sollten automatische Upgrades auf Hauptversionen aktiviert sein](#)
- [\[Redshift.7\] Redshift-Cluster sollten erweitertes VPC-Routing verwenden](#)
- [\[Redshift.8\] Amazon Redshift Redshift-Cluster sollten nicht den standardmäßigen Admin-Benutzernamen verwenden](#)
- [\[Redshift.9\] Redshift-Cluster sollten nicht den Standard-Datenbanknamen verwenden](#)
- [\[Redshift.10\] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[RedshiftServerless.4\] Serverlose Redshift-Namespaces sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys](#)
- [\[RedshiftServerless.7\] Redshift Serverless-Namespaces sollten nicht den Standard-Datenbanknamen verwenden](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.1\] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein](#)
- [\[S3.2\] S3-Allzweck-Buckets sollten den öffentlichen Lesezugriff blockieren](#)
- [\[S3.3\] S3-Allzweck-Buckets sollten den öffentlichen Schreibzugriff blockieren](#)
- [\[S3.5\] S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erfordern](#)

- [\[S3.6\] Allgemeine S3-Bucket-Richtlinien sollten den Zugriff auf andere einschränken AWS-Konten](#)
- [\[S3.7\] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden](#)
- [\[S3.8\] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren](#)
- [\[S3.9\] Bei S3-Allzweck-Buckets sollte die Serverzugriffsprotokollierung aktiviert sein](#)
- [\[S3.10\] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben](#)
- [\[S3.11\] Bei S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein](#)
- [\[S3.12\] ACLs sollte nicht zur Verwaltung des Benutzerzugriffs auf S3-Allzweck-Buckets verwendet werden](#)
- [\[S3.13\] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben](#)
- [\[S3.14\] Für S3-Allzweck-Buckets sollte die Versionierung aktiviert sein](#)
- [\[S3.15\] Bei S3-Allzweck-Buckets sollte Object Lock aktiviert sein](#)
- [\[S3.17\] S3-Allzweck-Buckets sollten im Ruhezustand verschlüsselt werden mit AWS KMS keys](#)
- [\[S3.19\] Bei S3-Zugriffspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.20\] Bei S3-Allzweck-Buckets sollte MFA Delete aktiviert sein](#)
- [\[SageMaker.1\] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben](#)
- [\[SageMaker.2\] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden](#)
- [\[SageMaker.3\] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben](#)
- [\[SageMaker.4\] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein](#)
- [\[SecretsManager.1\] Bei Secrets Manager Manager-Geheimnissen sollte die automatische Rotation aktiviert sein](#)
- [\[SecretsManager.2\] Secrets Manager Manager-Geheimnisse, die mit automatischer Rotation konfiguriert sind, sollten erfolgreich rotieren](#)
- [\[SecretsManager.3\] Unbenutzte Secrets Manager Manager-Geheimnisse entfernen](#)
- [\[SecretsManager.4\] Secrets Manager Manager-Geheimnisse sollten innerhalb einer bestimmten Anzahl von Tagen rotiert werden](#)
- [\[ServiceCatalog.1\] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden](#)

- [\[SNS.1\] SNS-Themen sollten im Ruhezustand wie folgt verschlüsselt werden AWS KMS](#)
- [\[SQS.1\] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt werden](#)
- [\[SSM.1\] EC2 Amazon-Instances sollten verwaltet werden von AWS Systems Manager](#)
- [\[SSM.2\] Von Systems Manager verwaltete EC2 Amazon-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben](#)
- [\[SSM.3\] Von Systems Manager verwaltete EC2 Amazon-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben](#)
- [\[SSM.4\] SSM-Dokumente sollten nicht öffentlich sein](#)
- [\[Transfer.2\] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden](#)
- [\[Transfer.3\] Bei Connectoren der Transfer-Familie sollte die Protokollierung aktiviert sein](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.2\] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.3\] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.4\] AWS WAF Classic Regional Web ACLs sollte mindestens eine Regel oder Regelgruppe enthalten](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WAF.10\] AWS WAF web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WAF.11\] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein](#)
- [Für \[WAF.12\] AWS WAF Regeln sollten Metriken aktiviert sein CloudWatch](#)

NIST SP 800-171 Revision 2 im Security Hub CSPM

Die NIST-Sonderveröffentlichung 800-171 Revision 2 (NIST SP 800-171 Rev. 2) ist ein Framework für Cybersicherheit und Compliance, das vom National Institute of Standards and Technology (NIST), einer Behörde, die Teil des US-Handelsministeriums ist, entwickelt wurde. Dieses Compliance-Framework enthält empfohlene Sicherheitsanforderungen für den Schutz der Vertraulichkeit kontrollierter, nicht klassifizierter Informationen in Systemen und Organisationen, die nicht Teil der

US-Bundesregierung sind. Kontrollierte, nicht klassifizierte Informationen, auch CUI genannt, sind vertrauliche Informationen, die nicht den staatlichen Klassifizierungskriterien entsprechen, aber geschützt werden müssen. Es handelt sich um Informationen, die als sensibel gelten und von der US-Bundesregierung oder anderen Stellen im Auftrag der US-Bundesregierung erstellt oder in Besitz genommen wurden.

NIST SP 800-171 Rev. 2 enthält empfohlene Sicherheitsanforderungen zum Schutz der Vertraulichkeit von CUI in folgenden Fällen:

- Die Informationen befinden sich in nichtföderalen Systemen und Organisationen,
- Die nichtföderale Organisation sammelt oder verwaltet keine Informationen im Auftrag einer Bundesbehörde und nutzt oder betreibt kein System im Auftrag einer Behörde, und
- Für die CUI-Kategorie, die im CUI-Register aufgeführt ist, gibt es keine spezifischen Schutzanforderungen zum Schutz der Vertraulichkeit von CUI, die in den Genehmigungsgesetzen, Verordnungen oder behördlichen Richtlinien vorgeschrieben sind.

Die Anforderungen gelten für alle Komponenten nichtstaatlicher Systeme und Organisationen, die CUI verarbeiten, speichern oder übertragen oder Sicherheitsschutz für die Komponenten bieten. Weitere Informationen finden Sie unter [NIST SP 800-171 Rev. 2](#) im NIST Computer Security Resource Center.

AWS Security Hub Cloud Security Posture Management (CSPM) bietet Sicherheitskontrollen, die einen Teil der Anforderungen von NIST SP 800-171 Revision 2 unterstützen. Die Kontrollen führen automatisierte Sicherheitsprüfungen für bestimmte Ressourcen durch. AWS-Services Um diese Kontrollen zu aktivieren und zu verwalten, können Sie das NIST SP 800-171 Revision 2-Framework standardmäßig in Security Hub CSPM aktivieren. Beachten Sie, dass die Steuerungen die Anforderungen von NIST SP 800-171 Revision 2, die manuelle Prüfungen erfordern, nicht unterstützen.

Themen

- [Konfiguration der Ressourcenaufzeichnung für Kontrollen, die für den Standard gelten](#)
- [Festlegung, welche Kontrollen für den Standard gelten](#)

Konfiguration der Ressourcenaufzeichnung für Kontrollen, die für den Standard gelten

Um die Abdeckung und die Genauigkeit der Ergebnisse zu optimieren, ist es wichtig, die Ressourcenaufzeichnung zu aktivieren und zu konfigurieren, AWS Config bevor Sie den Standard

NIST SP 800-171 Revision 2 in AWS Security Hub Cloud Security Posture Management (CSPM) aktivieren. Achten Sie bei der Konfiguration der Ressourcenaufzeichnung auch darauf, sie für alle AWS Ressourcentypen zu aktivieren, die durch die für den Standard geltenden Kontrollen überprüft werden. Andernfalls ist Security Hub CSPM möglicherweise nicht in der Lage, die geeigneten Ressourcen zu bewerten und genaue Ergebnisse für Kontrollen zu generieren, die für den Standard gelten.

Informationen darüber, wie Security Hub CSPM die Ressourcenaufzeichnung in verwendet AWS Config, finden Sie unter [Aktivierung und Konfiguration AWS Config für Security Hub CSPM](#). Informationen zur Konfiguration der Ressourcenaufzeichnung in AWS Config finden Sie unter [Arbeiten mit dem Konfigurationsrekorder](#) im AWS Config Entwicklerhandbuch.

In der folgenden Tabelle sind die Ressourcentypen aufgeführt, die für Kontrollen aufgezeichnet werden müssen, die für den Standard NIST SP 800-171 Revision 2 in Security Hub CSPM gelten.

AWS-Service	Ressourcentypen
AWS Certificate Manager(ACM)	AWS::ACM::Certificate
Amazon API Gateway	AWS::ApiGateway::Stage
Amazon CloudFront	AWS::CloudFront::Distribution
Amazon CloudWatch	AWS::CloudWatch::Alarm
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::ClientVpnEndpoint , AWS::EC2::NetworkAcl , AWS::EC2:: SecurityGroup , AWS::EC2::VPC , AWS::EC2::VPNConnection
Elastic Load Balancing	AWS::ElasticLoadBalancing:: LoadBalancer
AWS Identity and Access Management(IAM)	AWS::IAM::Policy , AWS::IAM::User
AWS Key Management Service (AWS KMS)	AWS::KMS::Alias , AWS::KMS::Key
AWS Network Firewall	AWS::NetworkFirewall::Firew allPolicy , AWS::NetworkFirewa ll::RuleGroup

AWS-Service	Ressourcentypen
Amazon Simple Storage Service (Amazon S3)	AWS::S3::Bucket
Amazon Simple Notification Service (Amazon SNS)	AWS::SNS::Topic
AWS Systems Manager(SSM)	AWS::SSM::PatchCompliance
AWS WAF	AWS::WAFv2::RuleGroup

Festlegung, welche Kontrollen für den Standard gelten

In der folgenden Liste sind die Kontrollen aufgeführt, die die Anforderungen von NIST SP 800-171 Revision 2 unterstützen und für den Standard NIST SP 800-171 Revision 2 in AWS Security Hub Cloud Security Posture Management (CSPM) gelten. Einzelheiten zu den spezifischen Anforderungen, die ein Steuerelement unterstützt, erhalten Sie, wenn Sie das Steuerelement auswählen. Weitere Informationen finden Sie in den Details für das Steuerelement im Feld „Verwandte Anforderungen“. Dieses Feld gibt jede NIST-Anforderung an, die das Steuerelement unterstützt. Wenn das Feld keine bestimmte NIST-Anforderung spezifiziert, unterstützt das Steuerelement die Anforderung nicht.

- [\[ACM.1\] Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden](#)
- [\[APIGateway.2\] API Gateway REST API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudTrail.2\] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben](#)
- [\[CloudTrail.3\] Mindestens ein CloudTrail Trail sollte aktiviert sein](#)
- [\[CloudTrail.4\] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein](#)
- [\[CloudWatch.1\] Für den Benutzer „root“ sollten ein Filter und ein Alarm für die Log-Metrik vorhanden sein](#)
- [\[CloudWatch.2\] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für nicht autorisierte API-Aufrufe vorhanden sind](#)

- [\[CloudWatch.4\] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der IAM-Richtlinie vorhanden sind](#)
- [\[CloudWatch.5\] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für CloudTrail -Config--Config-Änderungen vorhanden sind](#)
- [\[CloudWatch.6\] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für AWS Management Console Authentifizierungsfehler vorhanden sind](#)
- [\[CloudWatch.7\] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden verwalteten Schlüsseln vorhanden sind](#)
- [\[CloudWatch.8\] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der S3-Bucket-Richtlinie vorhanden sind](#)
- [\[CloudWatch.9\] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für AWS Config -Config--Config-Änderungen vorhanden sind](#)
- [\[CloudWatch.10\] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Sicherheitsgruppe vorhanden sind](#)
- [\[CloudWatch.11\] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an den Network Access Control Lists \(NACL\) vorhanden sind](#)
- [\[CloudWatch.12\] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an Network-Gateways vorhanden sind](#)
- [\[CloudWatch.13\] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Routing-Tabelle vorhanden sind](#)
- [\[CloudWatch.14\] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für VPC-Änderungen vorhanden sind](#)
- [\[CloudWatch.15\] Für CloudWatch Alarmer sollten bestimmte Aktionen konfiguriert sein](#)
- [\[EC2.6\] Die VPC-Flow-Protokollierung sollte in allen aktiviert sein VPCs](#)
- [\[EC2.10\] Amazon EC2 sollte so konfiguriert sein, dass es VPC-Endpunkte verwendet, die für den Amazon-Service erstellt wurden EC2](#)
- [\[EC2.13\] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen](#)
- [\[EC2.16\] Ungenutzte Network Access Control Lists sollten entfernt werden](#)
- [\[EC2.18\] Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Datenverkehr für autorisierte Ports zulassen](#)
- [\[EC2.19\] Sicherheitsgruppen sollten keinen uneingeschränkten Zugriff auf Ports mit hohem Risiko zulassen](#)

- [\[EC2.20\] Beide VPN-Tunnel für eine AWS Site-to-Site VPN-Verbindung sollten aktiv sein](#)
- [\[EC2.21\] Das Netzwerk ACLs sollte keinen Zugang von 0.0.0.0/0 zu Port 22 oder Port 3389 zulassen](#)
- [\[EC2.51\] EC2 Client-VPN-Endpunkte sollten die Client-Verbindungsprotokollierung aktiviert haben](#)
- [\[ELB.2\] Classic Load Balancer mit SSL/HTTPS Listnern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager](#)
- [\[ELB.3\] Classic Load Balancer Balancer-Listener sollten mit HTTPS- oder TLS-Terminierung konfiguriert werden](#)
- [\[ELB.8\] Classic Load Balancer mit SSL-Listnern sollten eine vordefinierte Sicherheitsrichtlinie mit starker Dauer verwenden AWS Config](#)
- [\[GuardDuty.1\] GuardDuty sollte aktiviert sein](#)
- [\[IAM.1\] IAM-Richtlinien sollten keine vollen „*“-Administratorrechte zulassen](#)
- [\[IAM.2\] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein](#)
- [\[IAM.7\] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein](#)
- [\[IAM.8\] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden](#)
- [\[IAM.10\] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein](#)
- [\[IAM.11\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert](#)
- [\[IAM.12\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert](#)
- [\[IAM.13\] Stellen Sie sicher, dass für die IAM-Passwortrichtlinie mindestens ein Symbol erforderlich ist](#)
- [\[IAM.14\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert](#)
- [\[IAM.15\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert](#)
- [\[IAM.16\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert](#)
- [\[IAM.18\] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS -Support](#)
- [\[IAM.19\] MFA sollte für alle IAM-Benutzer aktiviert sein](#)
- [\[IAM.21\] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen](#)

- [\[IAM.22\] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden](#)
- [\[NetworkFirewall.2\] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein](#)
- [\[NetworkFirewall.3\] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet haben](#)
- [\[NetworkFirewall.5\] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ sein.](#)
- [\[NetworkFirewall.6\] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein](#)
- [\[S3.5\] S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erfordern](#)
- [\[S3.6\] Allgemeine S3-Bucket-Richtlinien sollten den Zugriff auf andere einschränken AWS-Konten](#)
- [\[S3.9\] Bei S3-Allzweck-Buckets sollte die Serverzugriffsprotokollierung aktiviert sein](#)
- [\[S3.11\] Bei S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein](#)
- [\[S3.14\] Für S3-Allzweck-Buckets sollte die Versionierung aktiviert sein](#)
- [\[S3.17\] S3-Allzweck-Buckets sollten im Ruhezustand verschlüsselt werden mit AWS KMS keys](#)
- [\[SNS.1\] SNS-Themen sollten im Ruhezustand wie folgt verschlüsselt werden AWS KMS](#)
- [\[SSM.2\] Von Systems Manager verwaltete EC2 Amazon-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben](#)
- [Für \[WAF.12\] AWS WAF Regeln sollten Metriken aktiviert sein CloudWatch](#)

PCI DSS im Security Hub CSPM

Der Payment Card Industry Data Security Standard (PCI DSS) ist ein Compliance-Framework eines Drittanbieters, das eine Reihe von Regeln und Richtlinien für den sicheren Umgang mit Kredit- und Debitkarteninformationen enthält. Der PCI Security Standards Council (SSC) erstellt und aktualisiert dieses Framework.

AWS Security Hub Cloud Security Posture Management (CSPM) bietet einen PCI-DSS-Standard, mit dem Sie die Einhaltung dieses Drittanbieter-Frameworks sicherstellen können. Sie können diesen Standard verwenden, um Sicherheitslücken in AWS Ressourcen zu entdecken, die Karteninhaberdaten verarbeiten. Wir empfehlen AWS-Konten, diesen Standard für Ressourcen zu aktivieren, die Karteninhaberdaten oder sensible Authentifizierungsdaten speichern, verarbeiten oder übertragen. Durch Prüfungen durch das PCI SSC wurde dieser Standard bestätigt.

Security Hub CSPM bietet Unterstützung für PCI DSS v3.2.1 und PCI DSS v4.0.1. Wir empfehlen die Verwendung von Version 4.0.1, um über bewährte Sicherheitsmethoden auf dem Laufenden

zu bleiben. Sie können beide Versionen des Standards gleichzeitig aktivieren. Informationen zur Aktivierung von Standards finden Sie unter [Einen Sicherheitsstandard aktivieren](#). Wenn Sie derzeit Version 3.2.1 verwenden, aber nur Version 4.0.1 verwenden möchten, aktivieren Sie die neuere Version, bevor Sie die ältere Version deaktivieren. Dadurch werden Lücken in Ihren Sicherheitsüberprüfungen vermieden. Wenn Sie die Security Hub CSPM-Integration mit verwenden AWS Organizations und v4.0.1 in mehreren Konten stapelweise aktivieren möchten, empfehlen wir, dafür die [zentrale Konfiguration](#) zu verwenden.

In den folgenden Abschnitten wird angegeben, welche Kontrollen für PCI DSS v3.2.1 und PCI DSS v4.0.1 gelten.

Kontrollen, die für PCI DSS v3.2.1 gelten

Die folgende Liste gibt an, welche Security Hub CSPM-Steuerelemente für PCI DSS v3.2.1 gelten. Um die Details eines Steuerelements zu überprüfen, wählen Sie das Steuerelement aus.

[\[AutoScaling.1\] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden](#)

[\[CloudTrail.2\] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben](#)

[\[CloudTrail.3\] Mindestens ein CloudTrail Trail sollte aktiviert sein](#)

[\[CloudTrail.4\] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein](#)

[\[CloudTrail.5\] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden](#)

[\[CloudWatch.1\] Für den Benutzer „root“ sollten ein Filter und ein Alarm für die Log-Metrik vorhanden sein](#)

[\[CodeBuild.1\] Das CodeBuild Bitbucket-Quell-Repository URLs sollte keine vertraulichen Anmeldeinformationen enthalten](#)

[\[CodeBuild.2\] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten](#)

[\[Config.1\] AWS Config sollte aktiviert sein und die serviceverknüpfte Rolle für die Ressourcenaufzeichnung verwenden](#)

[\[DMS.1\] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein](#)

[\[EC2.1\] Amazon EBS-Snapshots sollten nicht öffentlich wiederherstellbar sein](#)

[\[EC2.2\] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen](#)

[\[EC2.6\] Die VPC-Flow-Protokollierung sollte in allen aktiviert sein VPCs](#)

[\[EC2.12\] Unbenutztes Amazon EC2 EIPs sollte entfernt werden](#)

[\[EC2.13\] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen](#)

[\[ELB.1\] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden](#)

[\[ES.1\] Bei Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein](#)

[\[ES.2\] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein](#)

[\[GuardDuty.1\] GuardDuty sollte aktiviert sein](#)

[\[IAM.1\] IAM-Richtlinien sollten keine vollen „*“-Administratorrechte zulassen](#)

[\[IAM.2\] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein](#)

[\[IAM.4\] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren](#)

[\[IAM.6\] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.](#)

[\[IAM.8\] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden](#)

[\[IAM.9\] MFA sollte für den Root-Benutzer aktiviert sein](#)

[\[IAM.10\] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein](#)

[\[IAM.19\] MFA sollte für alle IAM-Benutzer aktiviert sein](#)

[\[KMS.4\] Die AWS KMS Schlüsselrotation sollte aktiviert sein](#)

[\[Lambda.1\] Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten](#)

[\[Lambda.3\] Lambda-Funktionen sollten sich in einer VPC befinden](#)

[Bei \[Opensearch.1\] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein](#)

[\[Opensearch.2\] OpenSearch -Domains sollten nicht öffentlich zugänglich sein](#)

[\[RDS.1\] Der RDS-Snapshot sollte privat sein](#)

[\[RDS.2\] RDS-DB-Instances sollten, wie in der Konfiguration festgelegt, den öffentlichen Zugriff verbieten PubliclyAccessible](#)

[\[Redshift.1\] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten](#)

[\[S3.1\] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein](#)

[\[S3.2\] S3-Allzweck-Buckets sollten den öffentlichen Lesezugriff blockieren](#)

[\[S3.3\] S3-Allzweck-Buckets sollten den öffentlichen Schreibzugriff blockieren](#)

[\[S3.5\] S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erfordern](#)

[\[S3.7\] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden](#)

[\[SageMaker.1\] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben](#)

[\[SSM.1\] EC2 Amazon-Instances sollten verwaltet werden von AWS Systems Manager](#)

[\[SSM.2\] Von Systems Manager verwaltete EC2 Amazon-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben](#)

[\[SSM.3\] Von Systems Manager verwaltete EC2 Amazon-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben](#)

Kontrollen, die für PCI DSS v4.0.1 gelten

Die folgende Liste gibt an, welche Security Hub CSPM-Steuerelemente für PCI DSS v4.0.1 gelten. Um die Details eines Steuerelements zu überprüfen, wählen Sie das Steuerelement aus.

[\[ACM.1\] Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden](#)

[\[ACM.2\] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden](#)

[\[APIGateway.9\] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein](#)

[\[AppSync.2\] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben](#)

[\[AutoScaling.3\] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2 Instances so konfigurieren, dass sie Instance Metadata Service Version 2 \(IMDSv2\) benötigen](#)

[\[Autoscaling.5\] EC2 Amazon-Instances, die mit Auto Scaling Scaling-Gruppenstartkonfigurationen gestartet wurden, sollten keine öffentlichen IP-Adressen haben](#)

[Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)

[\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)

[\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)

[\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)

[\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)

[\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)

[\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)

[\[CloudTrail.2\] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben](#)

[\[CloudTrail.3\] Mindestens ein CloudTrail Trail sollte aktiviert sein](#)

[\[CloudTrail.4\] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein](#)

[\[CloudTrail.6\] Sicherstellen, dass der S3-Bucket, in dem CloudTrail Protokolle gespeichert werden, nicht öffentlich zugänglich ist](#)

[\[CloudTrail.7\] Sicherstellen, dass die S3-Bucket-Zugriffsprotokollierung für den CloudTrail S3-Bucket aktiviert ist](#)

[\[CodeBuild.1\] Das CodeBuild Bitbucket-Quell-Repository URLs sollte keine vertraulichen Anmeldeinformationen enthalten](#)

[\[CodeBuild.2\] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten](#)

[\[CodeBuild.3\] CodeBuild S3-Protokolle sollten verschlüsselt sein](#)

[\[DMS.1\] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein](#)

[\[DMS.10\] Bei DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein](#)

[\[DMS.11\] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein](#)

[\[DMS.12\] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein](#)

[\[DMS.6\] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein](#)

[\[DMS.7\] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein](#)

[\[DMS.8\] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein](#)

[\[DMS.9\] DMS-Endpunkte sollten SSL verwenden](#)

[\[DocumentDB.2\] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen](#)

[\[DocumentDB.3\] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein](#)

[\[DocumentDB.4\] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch](#)

[\[DynamoDB.7\] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden](#)

[\[EC2.13\] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen](#)

[\[EC2.14\] Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 oder: :/0 auf Port 3389 zulassen](#)

[\[EC2.15\] EC2 Amazon-Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen](#)

[\[EC2.16\] Ungenutzte Network Access Control Lists sollten entfernt werden](#)

[\[EC2.170\] EC2 Startvorlagen sollten Instance Metadata Service Version 2 \(\) verwenden IMDSv2](#)

[\[EC2.171\] Bei EC2 VPN-Verbindungen sollte die Protokollierung aktiviert sein](#)

[\[EC2.21\] Das Netzwerk ACLs sollte keinen Zugang von 0.0.0.0/0 zu Port 22 oder Port 3389 zulassen](#)

[\[EC2.25\] EC2 Amazon-Startvorlagen sollten Netzwerkschnittstellen nicht öffentlich IPs zuweisen](#)

- [\[EC2.51\] EC2 Client-VPN-Endpunkte sollten die Client-Verbindungsprotokollierung aktiviert haben](#)
- [\[EC2.53\] EC2 Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 zu Remote-Serververwaltungsports zulassen](#)
- [\[EC2.54\] EC2 Sicherheitsgruppen sollten keinen Zugriff von: :/0 zu Remote-Serveradministrationsports zulassen](#)
- [\[EC2.8\] EC2 Instances sollten Instance Metadata Service Version 2 \(\) verwenden IMDSv2](#)
- [\[ECR.1\] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein](#)
- [\[ECS.10\] Die ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen](#)
- [\[ECS.16\] ECS-Aufgabensätze sollten öffentliche IP-Adressen nicht automatisch zuweisen](#)
- [\[ECS.2\] ECS-Diensten sollten nicht automatisch öffentliche IP-Adressen zugewiesen werden](#)
- [\[ECS.8\] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden](#)
- [\[EFS.4\] EFS-Zugangspunkte sollten eine Benutzeridentität erzwingen](#)
- [\[EKS.1\] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein](#)
- [\[EKS.2\] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden](#)
- [\[EKS.3\] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden](#)
- [\[EKS.8\] Bei EKS-Clustern sollte die Auditprotokollierung aktiviert sein](#)
- [\[ElastiCache.2\] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein](#)
- [\[ElastiCache.5\] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden](#)
- [\[ElastiCache.6\] Für Replikationsgruppen ElastiCache \(Redis OSS\) früherer Versionen sollte Redis OSS AUTH aktiviert sein](#)
- [\[ElasticBeanstalk.2\] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk sollte Logs streamen nach CloudWatch](#)
- [\[ELB.12\] Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden](#)

[ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden

[ELB.3] Classic Load Balancer Balancer-Listener sollten mit HTTPS- oder TLS-Terminierung konfiguriert werden

[ELB.4] Application Load Balancer sollte so konfiguriert sein, dass ungültige HTTP-Header gelöscht werden

[ELB.8] Classic Load Balancer mit SSL-Listnern sollten eine vordefinierte Sicherheitsrichtlinie mit starker Dauer verwenden AWS Config

[EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben

[EMR.2] Die Amazon EMR-Einstellung zum Blockieren des öffentlichen Zugriffs sollte aktiviert sein

[ES.2] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein

[ES.3] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden

[ES.5] Für Elasticsearch-Domains sollte die Audit-Protokollierung aktiviert sein

[ES.8] Verbindungen zu Elasticsearch-Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden

[EventBridge.3] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden

[GuardDuty.1] GuardDuty sollte aktiviert sein

[GuardDuty.10] Der GuardDuty S3-Schutz sollte aktiviert sein

[GuardDuty.6] GuardDuty Lambda Protection sollte aktiviert sein

[GuardDuty.7] GuardDuty EKS Runtime Monitoring sollte aktiviert sein

[GuardDuty.9] Der GuardDuty RDS-Schutz sollte aktiviert sein

[IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden

[IAM.5] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen

[\[IAM.6\] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.](#)

[\[IAM.7\] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein](#)

[\[IAM.8\] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden](#)

[\[IAM.9\] MFA sollte für den Root-Benutzer aktiviert sein](#)

[\[IAM.11\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert](#)

[\[IAM.12\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert](#)

[\[IAM.14\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert](#)

[\[IAM.16\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert](#)

[\[IAM.17\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft](#)

[\[IAM.18\] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS -Support](#)

[\[IAM.19\] MFA sollte für alle IAM-Benutzer aktiviert sein](#)

[\[Inspector.1\] Das EC2 Scannen mit Amazon Inspector sollte aktiviert sein](#)

[\[Inspector.2\] Das Amazon Inspector ECR-Scannen sollte aktiviert sein](#)

[\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)

[\[Inspector.4\] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein](#)

[\[KMS.4\] Die AWS KMS Schlüsselrotation sollte aktiviert sein](#)

[\[Lambda.1\] Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten](#)

[\[Lambda.2\] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden](#)

[\[MQ.2\] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch](#)

[\[MQ.3\] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein](#)

[\[MSK.1\] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden](#)

[\[MSK.3\] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden](#)

[\[Neptune.2\] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)

[\[Neptune.3\] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein](#)

[Auf \[Opensearch.10\] OpenSearch -Domains sollte das neueste Softwareupdate installiert sein](#)

[Für \[Opensearch.5\] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein](#)

[\[RDS.13\] Automatische RDS-Upgrades für Nebenversionen sollten aktiviert sein](#)

[\[RDS.2\] RDS-DB-Instances sollten, wie in der Konfiguration festgelegt, den öffentlichen Zugriff verbieten PubliclyAccessible](#)

[\[RDS.20\] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Ereignisse der Datenbankinstanz konfiguriert werden](#)

[\[RDS.21\] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbankparametergruppenereignisse konfiguriert werden](#)

[\[RDS.22\] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbanksicherheitsgruppenereignisse konfiguriert werden](#)

[\[RDS.24\] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden](#)

[\[RDS.25\] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden](#)

[\[RDS.34\] Aurora MySQL-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)

[\[RDS.35\] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein](#)

[\[RDS.36\] RDS für PostgreSQL-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch](#)

[\[RDS.37\] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch](#)

[\[RDS.9\] RDS-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch](#)

[\[Redshift.1\] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten](#)

[Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen

[Redshift.2] Verbindungen zu Amazon Redshift Redshift-Clustern sollten bei der Übertragung verschlüsselt werden

[Redshift.4] Bei Amazon Redshift Redshift-Clustern sollte die Auditprotokollierung aktiviert sein

[Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren

[S3.1] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein

[S3.15] Bei S3-Allzweck-Buckets sollte Object Lock aktiviert sein

[S3.17] S3-Allzweck-Buckets sollten im Ruhezustand verschlüsselt werden mit AWS KMS keys

[S3.19] Bei S3-Zugriffspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein

[S3.22] S3-Allzweck-Buckets sollten Schreibereignisse auf Objektebene protokollieren

[S3.23] S3-Allzweck-Buckets sollten Leseereignisse auf Objektebene protokollieren

[S3.24] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein

[S3.5] S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erfordern

[S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren

[S3.9] Bei S3-Allzweck-Buckets sollte die Serverzugriffsprotokollierung aktiviert sein

[SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben

[SecretsManager.1] Bei Secrets Manager Manager-Geheimnissen sollte die automatische Rotation aktiviert sein

[SecretsManager.2] Secrets Manager Manager-Geheimnisse, die mit automatischer Rotation konfiguriert sind, sollten erfolgreich rotieren

[SecretsManager.4] Secrets Manager Manager-Geheimnisse sollten innerhalb einer bestimmten Anzahl von Tagen rotiert werden

[\[SSM.2\] Von Systems Manager verwaltete EC2 Amazon-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben](#)

[\[SSM.3\] Von Systems Manager verwaltete EC2 Amazon-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben](#)

[\[StepFunctions.1\] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben](#)

[\[Transfer.2\] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden](#)

[\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)

[\[WAF.11\] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein](#)

Von Diensten verwaltete Standards in Security Hub CSPM

Ein vom Service verwalteter Standard ist ein Sicherheitsstandard, der von einem anderen AWS-Service verwaltet wird, den Sie jedoch in Security Hub CSPM einsehen können. Zum Beispiel ist [Service-Managed Standard: ein vom Service verwalteter Standard](#), der verwaltet AWS Control Tower wird. AWS Control Tower Ein Service-Managed-Standard unterscheidet sich von einem Sicherheitsstandard, den AWS Security Hub Cloud Security Posture Management (CSPM) auf folgende Weise verwaltet:

- **Erstellung und Löschung von Standards** — Sie erstellen und löschen einen vom Service verwalteten Standard mit der Konsole oder API des verwaltenden Dienstes oder mit dem. AWS CLI Solange Sie den Standard nicht auf eine dieser Arten im Verwaltungsdienst erstellt haben, wird der Standard nicht in der Security Hub CSPM-Konsole angezeigt und ist nicht über die Security Hub CSPM-API zugänglich oder. AWS CLI
- **Keine automatische Aktivierung von Kontrollen** — Wenn Sie einen vom Service verwalteten Standard erstellen, aktivieren Security Hub CSPM und der Verwaltungsdienst nicht automatisch die Kontrollen, die für den Standard gelten. Wenn Security Hub CSPM neue Kontrollen für den Standard veröffentlicht, werden diese außerdem nicht automatisch aktiviert. Dies ist eine Abkehr von den Standards, die Security Hub CSPM verwaltet. Weitere Informationen zur üblichen Konfiguration von Steuerelementen in Security Hub CSPM finden Sie unter. [Grundlegendes zu den Sicherheitskontrollen in Security Hub CSPM](#)
- **Steuerungen aktivieren und deaktivieren** — Wir empfehlen, die Steuerungen im Verwaltungsdienst zu aktivieren und zu deaktivieren, um Abweichungen zu vermeiden.

- Verfügbarkeit von Kontrollen — Der Verwaltungsdienst entscheidet, welche Kontrollen im Rahmen des vom Service verwalteten Standards verfügbar sind. Die verfügbaren Kontrollen können alle oder einen Teil der vorhandenen Security Hub CSPM-Steuerelemente umfassen.

Nachdem der Verwaltungsdienst den vom Service verwalteten Standard erstellt und Kontrollen dafür verfügbar gemacht hat, können Sie in der Security Hub CSPM-Konsole, der Security Hub CSPM-API oder auf Ihre Kontrollergebnisse, Kontrollstatus und Standardsicherheitsbewertung zugreifen. AWS CLI Einige oder alle dieser Informationen sind möglicherweise auch im Verwaltungsdienst verfügbar.

Wählen Sie einen vom Service verwalteten Standard aus der folgenden Liste aus, um weitere Informationen zu diesem Standard zu erhalten.

Vom Service verwaltete Standards

- [Vom Service verwalteter Standard: AWS Control Tower](#)

Vom Service verwalteter Standard: AWS Control Tower

Dieser Abschnitt enthält Informationen zum Service-Managed Standard: AWS Control Tower

Was ist Service-Managed Standard? AWS Control Tower

Dieser Standard richtet sich an Benutzer von AWS Security Hub Cloud Security Posture Management (CSPM) und AWS Control Tower. Damit können Sie die proaktiven Kontrollen AWS Control Tower neben den detektiven Kontrollen von Security Hub CSPM im AWS Control Tower Service konfigurieren.

Proaktive Kontrollen tragen dazu bei, dass Sie die Vorschriften AWS-Konten einhalten, da sie Aktionen kennzeichnen, die zu Richtlinienverstößen oder Fehlkonfigurationen führen können. Detective Controls erkennt die Nichtkonformität von Ressourcen (z. B. Fehlkonfigurationen) in Ihrem AWS-Konten. Indem Sie proaktive und detektive Kontrollen für Ihre AWS Umgebung aktivieren, können Sie Ihre Sicherheitslage in verschiedenen Entwicklungsphasen verbessern.

Tip

Service-verwaltete Standards unterscheiden sich von den Standards, die AWS Security Hub Cloud Security Posture Management (CSPM) verwaltet. Beispielsweise müssen Sie im Verwaltungsdienst einen vom Dienst verwalteten Standard erstellen und löschen. Weitere Informationen finden Sie unter [Von Diensten verwaltete Standards in Security Hub CSPM](#).

In der Security Hub CSPM-Konsole und API können Sie Service-Managed Standard: AWS Control Tower zusammen mit anderen Security Hub CSPM-Standards anzeigen.

Den Standard erstellen

Dieser Standard ist nur verfügbar, wenn Sie den Standard in erstellen AWS Control Tower. AWS Control Tower erstellt den Standard, wenn Sie ein entsprechendes Steuerelement zum ersten Mal mithilfe einer der folgenden Methoden aktivieren:

- AWS Control Tower Konsole
- AWS Control Tower API (rufen Sie die [EnableControl](#)API auf)
- AWS CLI (führe den [enable-control](#)Befehl aus)

Security Hub CSPM-Steuerelemente werden in der AWS Control Tower Konsole als SH identifiziert. *ControlID*(zum Beispiel SH. CodeBuild.1).

Wenn Sie den Standard erstellen und Security Hub CSPM noch nicht aktiviert haben, aktiviert er AWS Control Tower auch Security Hub CSPM für Sie.

Wenn Sie ihn nicht eingerichtet haben AWS Control Tower, können Sie diesen Standard in der Security Hub CSPM-Konsole, der Security Hub CSPM-API oder nicht anzeigen oder darauf zugreifen. AWS CLI Selbst wenn Sie ihn eingerichtet haben AWS Control Tower, können Sie diesen Standard in Security Hub CSPM nicht anzeigen oder darauf zugreifen, ohne den Standard zuerst AWS Control Tower mit einer der oben genannten Methoden zu erstellen.

Dieser Standard ist nur in den Bereichen verfügbar, in [AWS-Regionen denen er verfügbar AWS Control Tower ist, einschließlich](#). AWS GovCloud (US)

Steuerungen im Standard aktivieren und deaktivieren

Nachdem Sie den Standard in der AWS Control Tower Konsole erstellt haben, können Sie den Standard und die verfügbaren Steuerelemente in beiden Diensten anzeigen.

Nachdem Sie den Standard zum ersten Mal erstellt haben, enthält er keine Steuerelemente, die automatisch aktiviert werden. Wenn Security Hub CSPM neue Steuerelemente hinzufügt, werden diese außerdem nicht automatisch für Service-Managed Standard: aktiviert. AWS Control Tower Sie sollten die Kontrollen für den Standard aktivieren und deaktivieren, AWS Control Tower indem Sie eine der folgenden Methoden verwenden:

- AWS Control Tower Konsole

- AWS Control Tower API (rufe das [EnableControl](#) und auf [DisableControl](#) APIs)
- AWS CLI (führe die [disable-control](#) Befehle [enable-control](#) und aus)

Wenn Sie den Aktivierungsstatus eines Steuerelements in ändern AWS Control Tower, spiegelt sich die Änderung auch in Security Hub CSPM wider.

Die Deaktivierung eines Steuerelements in Security Hub CSPM, das aktiviert ist, AWS Control Tower führt jedoch zu Kontrollabweichungen. Der Kontrollstatus in AWS Control Tower wird als angezeigt. Drifted Sie können diese Abweichung beheben, indem Sie in der AWS Control Tower Konsole die Option [OU erneut registrieren](#) auswählen oder die Steuerung AWS Control Tower mithilfe einer der oben genannten Methoden deaktivieren und erneut aktivieren.

Wenn Sie die Aktivierungs- und Deaktivierungsaktionen in abschließen, können Sie Kontrollabweichungen vermeiden. AWS Control Tower

Wenn Sie Kontrollen in aktivieren oder deaktivieren AWS Control Tower, gilt die Aktion für alle Konten und Regionen. Wenn Sie Kontrollen in Security Hub CSPM aktivieren und deaktivieren (für diesen Standard nicht empfohlen), gilt die Aktion nur für das aktuelle Konto und die Region.

Note

[Die zentrale Konfiguration](#) kann nicht zur Verwaltung von Service-Managed Standard: verwendet werden. AWS Control Tower Wenn Sie die zentrale Konfiguration verwenden, können Sie nur den AWS Control Tower Dienst verwenden, um die Steuerungen in diesem Standard für ein zentral verwaltetes Konto zu aktivieren und zu deaktivieren.

Aktivierungsstatus und Kontrollstatus anzeigen

Sie können den Aktivierungsstatus einer Kontrolle mit einer der folgenden Methoden anzeigen:

- Security Hub CSPM-Konsole, Security Hub CSPM-API oder AWS CLI
- AWS Control Tower Konsole
- AWS Control Tower API, um eine Liste der aktivierten Steuerelemente zu sehen (rufen Sie die [ListEnabledControls](#) API auf)
- AWS CLI um eine Liste der aktivierten Steuerelemente zu sehen (führen Sie den [list-enabled-controls](#) Befehl aus)

Ein Steuerelement, das Sie deaktivieren, AWS Control Tower hat den Aktivierungsstatus **Disabled** in Security Hub CSPM, sofern Sie dieses Steuerelement nicht explizit in Security Hub CSPM aktivieren.

Security Hub CSPM berechnet den Kontrollstatus auf der Grundlage des Workflow-Status und des Compliance-Status der Kontrollergebnisse. Weitere Informationen zum Aktivierungsstatus und zum Kontrollstatus finden Sie unter [Überprüfung der Details der Kontrollen in Security Hub CSPM](#)

Auf der Grundlage des Kontrollstatus berechnet Security Hub CSPM eine [Sicherheitsbewertung](#) für Service-Managed Standard:. AWS Control Tower Diese Bewertung ist nur in Security Hub CSPM verfügbar. Darüber hinaus können Sie [Kontrollergebnisse](#) nur in Security Hub CSPM anzeigen. Die Standard-Sicherheitsbewertung und die Kontrollergebnisse sind in nicht verfügbar. AWS Control Tower

 Note

Wenn Sie Kontrollen für Service-Managed Standard: aktivieren AWS Control Tower, kann es bis zu 18 Stunden dauern, bis Security Hub CSPM Ergebnisse für Kontrollen generiert, die eine bestehende AWS Config serviceverknüpfte Regel verwenden. Möglicherweise verfügen Sie bereits über serviceverknüpfte Regeln, wenn Sie andere Standards und Kontrollen in Security Hub CSPM aktiviert haben. Weitere Informationen finden Sie unter [Zeitplan für die Ausführung von Sicherheitsprüfungen](#).

Den Standard löschen

Sie können diesen Standard löschen, AWS Control Tower indem Sie alle entsprechenden Steuerelemente mit einer der folgenden Methoden deaktivieren:

- AWS Control Tower Konsole
- AWS Control Tower API (rufen Sie die [DisableControl](#)API auf)
- AWS CLI (führe den [disable-control](#)Befehl aus)

Durch das Deaktivieren aller Steuerelemente wird der Standard in allen verwalteten Konten und verwalteten Regionen in gelöscht. AWS Control Tower Wenn Sie den Standard-in löschen, wird er von der Seite Standards der Security Hub CSPM-Konsole AWS Control Tower entfernt, und Sie können nicht mehr mit der Security Hub CSPM-API darauf zugreifen oder. AWS CLI

 Note

Durch die Deaktivierung aller Steuerelemente aus dem Standard in Security Hub CSPM wird der Standard nicht deaktiviert oder gelöscht.

Durch die Deaktivierung des Security Hub CSPM-Dienstes werden Service-Managed Standard: AWS Control Tower und alle anderen Standards, die Sie aktiviert haben, entfernt.

Das Feldformat für Service-Managed Standard finden: AWS Control Tower

Wenn Sie Service-Managed Standard: erstellen AWS Control Tower und Kontrollen dafür aktivieren, erhalten Sie ab sofort Kontrollergebnisse in Security Hub CSPM. Security Hub CSPM meldet Kontrollergebnisse in der. [AWS Format für Sicherheitssuche \(ASFF\)](#) Dies sind die ASFF-Werte für den Amazon Resource Name (ARN) dieses Standards und `GeneratorId`:

- Standard-ARN — `arn:aws:us-east-1:securityhub:::standards/service-managed-aws-control-tower/v/1.0.0`
- `GeneratorId` – `service-managed-aws-control-tower/v/1.0.0/CodeBuild.1`

Ein Beispiel für einen Befund für Service-Managed Standard: finden Sie AWS Control Tower unter [Stichproben von Kontrollbefunden](#).

Kontrollen, die für Service-Managed Standard gelten: AWS Control Tower

Service-Managed Standard: AWS Control Tower unterstützt eine Teilmenge von Kontrollen, die Teil des FSBP-Standards (AWS Foundational Security Best Practices) sind. Wählen Sie ein Steuerelement aus, um Informationen darüber anzuzeigen, einschließlich Schritte zur Behebung fehlgeschlagener Ergebnisse.

Die folgende Liste zeigt die verfügbaren Steuerelemente für Service-Managed Standard: AWS Control Tower Die regionalen Grenzwerte für Kontrollen entsprechen den regionalen Grenzwerten für die entsprechenden Kontrollen im FSBP-Standard. Diese Liste zeigt standardunabhängige Sicherheitskontrollen. IDs In der AWS Control Tower Konsole IDs sind Steuerelemente als SH formatiert. **ControlID**(zum Beispiel SH. CodeBuild.1). Wenn in Security Hub CSPM [konsolidierte Kontrollergebnisse](#) in Ihrem Konto deaktiviert sind, verwendet das `ProductFields.ControlId` Feld die standardbasierte Kontroll-ID. Die standardbasierte Kontroll-ID ist als CT formatiert. **ControlId**(zum Beispiel CT. CodeBuild.1).

- [\[Account.1\] Sicherheitskontakthinformationen sollten bereitgestellt werden für AWS-Konto](#)
- [\[ACM.1\] Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden](#)
- [\[ACM.2\] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden](#)
- [\[APIGateway.1\] API Gateway REST und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein](#)
- [\[APIGateway.2\] API Gateway REST API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden](#)
- [\[APIGateway.3\] Bei den REST-API-Stufen von API Gateway sollte die AWS X-Ray Ablaufverfolgung aktiviert sein](#)
- [\[APIGateway.4\] API Gateway sollte mit einer WAF-Web-ACL verknüpft sein](#)
- [\[APIGateway.5\] API Gateway REST API-Cache-Daten sollten im Ruhezustand verschlüsselt werden](#)
- [\[APIGateway.8\] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben](#)
- [\[APIGateway.9\] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein](#)
- [\[AppSync.5\] AWS AppSync GraphQL APIs sollte nicht mit API-Schlüsseln authentifiziert werden](#)
- [\[AutoScaling.1\] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden](#)
- [\[AutoScaling.2\] Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken](#)
- [\[AutoScaling.3\] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2 Instances so konfigurieren, dass sie Instance Metadata Service Version 2 \(IMDSv2\) benötigen](#)
- [\[Autoscaling.5\] EC2 Amazon-Instances, die mit Auto Scaling Scaling-Gruppenstartkonfigurationen gestartet wurden, sollten keine öffentlichen IP-Adressen haben](#)
- [\[AutoScaling.6\] Auto Scaling Scaling-Gruppen sollten mehrere Instance-Typen in mehreren Availability Zones verwenden](#)
- [\[AutoScaling.9\] Amazon EC2 Auto Scaling Scaling-Gruppen sollten EC2 Amazon-Startvorlagen verwenden](#)
- [\[CloudTrail.1\] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst](#)
- [\[CloudTrail.2\] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben](#)
- [\[CloudTrail.4\] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein](#)

- [\[CloudTrail.5\] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden](#)
- [\[CloudTrail.6\] Sicherstellen, dass der S3-Bucket, in dem CloudTrail Protokolle gespeichert werden, nicht öffentlich zugänglich ist](#)
- [\[CodeBuild.1\] Das CodeBuild Bitbucket-Quell-Repository URLs sollte keine vertraulichen Anmeldeinformationen enthalten](#)
- [\[CodeBuild.2\] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten](#)
- [\[CodeBuild.3\] CodeBuild S3-Protokolle sollten verschlüsselt sein](#)
- [\[CodeBuild.4\] CodeBuild Projektumgebungen sollten eine AWS Config Protokollierungsdauer haben](#)
- [\[DMS.1\] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein](#)
- [\[DMS.9\] DMS-Endpunkte sollten SSL verwenden](#)
- [\[DocumentDB.1\] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DocumentDB.2\] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen](#)
- [\[DocumentDB.3\] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein](#)
- [\[DynamoDB.1\] DynamoDB-Tabellen sollten die Kapazität automatisch bei Bedarf skalieren](#)
- [\[DynamoDB.2\] Bei DynamoDB-Tabellen sollte die Wiederherstellung aktiviert sein point-in-time](#)
- [\[DynamoDB.3\] DynamoDB Accelerator \(DAX\) -Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[EC2.1\] Amazon EBS-Snapshots sollten nicht öffentlich wiederherstellbar sein](#)
- [\[EC2.2\] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen](#)
- [\[EC2.3\] Angehängte Amazon EBS-Volumes sollten im Ruhezustand verschlüsselt werden](#)
- [\[EC2.4\] Gestoppte EC2 Instances sollten nach einem bestimmten Zeitraum entfernt werden](#)
- [\[EC2.6\] Die VPC-Flow-Protokollierung sollte in allen aktiviert sein VPCs](#)
- [\[EC2.7\] Die EBS-Standardverschlüsselung sollte aktiviert sein](#)
- [\[EC2.8\] EC2 Instances sollten Instance Metadata Service Version 2 \(\) verwenden IMDSv2](#)
- [\[EC2.9\] EC2 Amazon-Instances sollten keine öffentliche IPv4 Adresse haben](#)
- [\[EC2.10\] Amazon EC2 sollte so konfiguriert sein, dass es VPC-Endpunkte verwendet, die für den Amazon-Service erstellt wurden EC2](#)

- [\[EC2.15\] EC2 Amazon-Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen](#)
- [\[EC2.16\] Ungenutzte Network Access Control Lists sollten entfernt werden](#)
- [\[EC2.17\] EC2 Amazon-Instances sollten nicht mehrere verwenden ENIs](#)
- [\[EC2.18\] Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Datenverkehr für autorisierte Ports zulassen](#)
- [\[EC2.19\] Sicherheitsgruppen sollten keinen uneingeschränkten Zugriff auf Ports mit hohem Risiko zulassen](#)
- [\[EC2.20\] Beide VPN-Tunnel für eine AWS Site-to-Site VPN-Verbindung sollten aktiv sein](#)
- [\[EC2.21\] Das Netzwerk ACLs sollte keinen Zugang von 0.0.0.0/0 zu Port 22 oder Port 3389 zulassen](#)
- [\[EC2.22\] Ungenutzte EC2 Amazon-Sicherheitsgruppen sollten entfernt werden](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways sollte VPC-Anhangsanfragen nicht automatisch akzeptieren](#)
- [\[EC2.25\] EC2 Amazon-Startvorlagen sollten Netzwerkschnittstellen nicht öffentlich IPs zuweisen](#)
- [\[ECR.1\] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein](#)
- [\[ECR.2\] Bei privaten ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein](#)
- [\[ECR.3\] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein](#)
- [\[ECS.1\] Amazon ECS-Aufgabendefinitionen sollten sichere Netzwerkmodi und Benutzerdefinitionen enthalten](#)
- [\[ECS.2\] ECS-Diensten sollten nicht automatisch öffentliche IP-Adressen zugewiesen werden](#)
- [\[ECS.3\] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen](#)
- [\[ECS.4\] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden](#)
- [\[ECS.5\] ECS-Container sollten auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sein](#)
- [\[ECS.8\] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden](#)
- [\[ECS.10\] Die ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen](#)
- [\[ECS.12\] ECS-Cluster sollten Container Insights verwenden](#)
- [\[EFS.1\] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS](#)
- [\[EFS.2\] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein](#)

- [\[EFS.3\] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen](#)
- [\[EFS.4\] EFS-Zugangspunkte sollten eine Benutzeridentität erzwingen](#)
- [\[EKS.1\] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein](#)
- [\[EKS.2\] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden](#)
- [\[ElastiCache.3\] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein](#)
- [\[ElastiCache.4\] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden](#)
- [\[ElastiCache.5\] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden](#)
- [\[ElastiCache.6\] Für Replikationsgruppen ElastiCache \(Redis OSS\) früherer Versionen sollte Redis OSS AUTH aktiviert sein](#)
- [\[ElasticBeanstalk.1\] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben](#)
- [\[ElasticBeanstalk.2\] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein](#)
- [\[ELB.1\] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden](#)
- [\[ELB.2\] Classic Load Balancer mit SSL/HTTPS Listnern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager](#)
- [\[ELB.3\] Classic Load Balancer Balancer-Listener sollten mit HTTPS- oder TLS-Terminierung konfiguriert werden](#)
- [\[ELB.4\] Application Load Balancer sollte so konfiguriert sein, dass ungültige HTTP-Header gelöscht werden](#)
- [\[ELB.5\] Die Protokollierung von Anwendungen und Classic Load Balancers sollte aktiviert sein](#)
- [\[ELB.6\] Für Anwendungen, Gateways und Network Load Balancers sollte der Löschschutz aktiviert sein](#)
- [\[ELB.7\] Bei Classic Load Balancers sollte der Verbindungsabbau aktiviert sein](#)
- [\[ELB.8\] Classic Load Balancer mit SSL-Listnern sollten eine vordefinierte Sicherheitsrichtlinie mit starker Dauer verwenden AWS Config](#)
- [\[ELB.9\] Bei Classic Load Balancers sollte der zonenübergreifende Load Balancing aktiviert sein](#)
- [\[ELB.10\] Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken](#)
- [\[ELB.12\] Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden](#)
- [\[ELB.13\] Anwendungs-, Netzwerk- und Gateway-Load Balancer sollten sich über mehrere Availability Zones erstrecken](#)

- [\[ELB.14\] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden](#)
- [\[EMR.1\] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben](#)
- [\[ES.1\] Bei Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein](#)
- [\[ES.2\] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein](#)
- [\[ES.3\] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden](#)
- [\[ES.4\] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein](#)
- [\[ES.5\] Für Elasticsearch-Domains sollte die Audit-Protokollierung aktiviert sein](#)
- [\[ES.6\] Elasticsearch-Domains sollten mindestens drei Datenknoten haben](#)
- [\[ES.7\] Elasticsearch-Domänen sollten mit mindestens drei dedizierten Master-Knoten konfiguriert werden](#)
- [\[ES.8\] Verbindungen zu Elasticsearch-Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden](#)
- [\[EventBridge.3\] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden](#)
- [\[GuardDuty.1\] GuardDuty sollte aktiviert sein](#)
- [\[IAM.1\] IAM-Richtlinien sollten keine vollen „*“-Administratorrechte zulassen](#)
- [\[IAM.2\] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein](#)
- [\[IAM.3\] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden](#)
- [\[IAM.4\] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren](#)
- [\[IAM.5\] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen](#)
- [\[IAM.6\] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.](#)
- [\[IAM.7\] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein](#)
- [\[IAM.8\] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden](#)
- [\[IAM.21\] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen](#)
- [\[Kinesis.1\] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden](#)
- [\[KMS.1\] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)
- [\[KMS.2\] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)

- [\[KMS.3\] AWS KMS keys sollte nicht unbeabsichtigt gelöscht werden](#)
- [\[KMS.4\] Die AWS KMS Schlüsselrotation sollte aktiviert sein](#)
- [\[Lambda.1\] Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten](#)
- [\[Lambda.2\] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden](#)
- [\[Lambda.3\] Lambda-Funktionen sollten sich in einer VPC befinden](#)
- [\[Lambda.5\] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren](#)
- [\[MSK.1\] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden](#)
- [\[MQ.5\] ActiveMQ-Broker sollten den Aktiv-/Standby-Bereitstellungsmodus verwenden](#)
- [\[MQ.6\] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden](#)
- [\[Neptune.1\] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.2\] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)
- [\[Neptune.3\] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein](#)
- [\[Neptune.4\] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[Neptune.5\] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein](#)
- [\[Neptune.6\] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.7\] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein](#)
- [\[Neptune.8\] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren](#)
- [\[NetworkFirewall.3\] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet haben](#)
- [\[NetworkFirewall.4\] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ sein.](#)
- [\[NetworkFirewall.5\] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ sein.](#)
- [\[NetworkFirewall.6\] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein](#)
- [Bei \[Opensearch.1\] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein](#)
- [\[Opensearch.2\] OpenSearch -Domains sollten nicht öffentlich zugänglich sein](#)
- [\[Opensearch.3\] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden](#)
- [Die Protokollierung von \[Opensearch.4\] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein](#)

- [Für \[Opensearch.5\] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein](#)
- [\[Opensearch.6\] OpenSearch Domains sollten mindestens drei Datenknoten haben](#)
- [Für \[Opensearch.7\] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein](#)
- [\[Opensearch.8\] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden](#)
- [\[RDS.1\] Der RDS-Snapshot sollte privat sein](#)
- [\[RDS.2\] RDS-DB-Instances sollten, wie in der Konfiguration festgelegt, den öffentlichen Zugriff verbieten PubliclyAccessible](#)
- [\[RDS.3\] Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein.](#)
- [\[RDS.4\] RDS-Cluster-Snapshots und Datenbank-Snapshots sollten im Ruhezustand verschlüsselt werden](#)
- [\[RDS.5\] RDS-DB-Instances sollten mit mehreren Availability Zones konfiguriert werden](#)
- [\[RDS.6\] Die erweiterte Überwachung sollte für RDS-DB-Instances konfiguriert werden](#)
- [\[RDS.8\] Für RDS-DB-Instances sollte der Löschschutz aktiviert sein](#)
- [\[RDS.9\] RDS-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[RDS.10\] Die IAM-Authentifizierung sollte für RDS-Instances konfiguriert werden](#)
- [\[RDS.11\] Bei RDS-Instances sollten automatische Backups aktiviert sein](#)
- [\[RDS.12\] Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden](#)
- [\[RDS.13\] Automatische RDS-Upgrades für Nebenversionen sollten aktiviert sein](#)
- [\[RDS.15\] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden](#)
- [\[RDS.17\] RDS-DB-Instances sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren](#)
- [\[RDS.18\] RDS-Instances sollten in einer VPC bereitgestellt werden](#)
- [\[RDS.19\] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Cluster-Ereignisse konfiguriert werden](#)
- [\[RDS.20\] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Ereignisse der Datenbankinstanz konfiguriert werden](#)
- [\[RDS.21\] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbankparametergruppenereignisse konfiguriert werden](#)
- [\[RDS.22\] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbanksicherheitsgruppenereignisse konfiguriert werden](#)
- [\[RDS.23\] RDS-Instances sollten keinen Standard-Port für die Datenbank-Engine verwenden](#)

- [\[RDS.25\] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden](#)
- [\[RDS.27\] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[Redshift.1\] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten](#)
- [\[Redshift.2\] Verbindungen zu Amazon Redshift Redshift-Clustern sollten bei der Übertragung verschlüsselt werden](#)
- [\[Redshift.4\] Bei Amazon Redshift Redshift-Clustern sollte die Auditprotokollierung aktiviert sein](#)
- [\[Redshift.6\] Bei Amazon Redshift sollten automatische Upgrades auf Hauptversionen aktiviert sein](#)
- [\[Redshift.7\] Redshift-Cluster sollten erweitertes VPC-Routing verwenden](#)
- [\[Redshift.8\] Amazon Redshift Redshift-Cluster sollten nicht den standardmäßigen Admin-Benutzernamen verwenden](#)
- [\[Redshift.9\] Redshift-Cluster sollten nicht den Standard-Datenbanknamen verwenden](#)
- [\[Redshift.10\] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[S3.1\] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein](#)
- [\[S3.2\] S3-Allzweck-Buckets sollten den öffentlichen Lesezugriff blockieren](#)
- [\[S3.3\] S3-Allzweck-Buckets sollten den öffentlichen Schreibzugriff blockieren](#)
- [\[S3.5\] S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erfordern](#)
- [\[S3.6\] Allgemeine S3-Bucket-Richtlinien sollten den Zugriff auf andere einschränken AWS-Konten](#)
- [\[S3.8\] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren](#)
- [\[S3.9\] Bei S3-Allzweck-Buckets sollte die Serverzugriffsprotokollierung aktiviert sein](#)
- [\[S3.12\] ACLs sollte nicht zur Verwaltung des Benutzerzugriffs auf S3-Allzweck-Buckets verwendet werden](#)
- [\[S3.13\] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben](#)
- [\[S3.17\] S3-Allzweck-Buckets sollten im Ruhezustand verschlüsselt werden mit AWS KMS keys](#)
- [\[SageMaker.1\] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben](#)
- [\[SageMaker.2\] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden](#)
- [\[SageMaker.3\] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben](#)
- [\[SecretsManager.1\] Bei Secrets Manager Manager-Geheimnissen sollte die automatische Rotation aktiviert sein](#)

- [\[SecretsManager.2\] Secrets Manager Manager-Geheimnisse, die mit automatischer Rotation konfiguriert sind, sollten erfolgreich rotieren](#)
- [\[SecretsManager.3\] Unbenutzte Secrets Manager Manager-Geheimnisse entfernen](#)
- [\[SecretsManager.4\] Secrets Manager Manager-Geheimnisse sollten innerhalb einer bestimmten Anzahl von Tagen rotiert werden](#)
- [\[SQS.1\] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt werden](#)
- [\[SSM.1\] EC2 Amazon-Instances sollten verwaltet werden von AWS Systems Manager](#)
- [\[SSM.2\] Von Systems Manager verwaltete EC2 Amazon-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben](#)
- [\[SSM.3\] Von Systems Manager verwaltete EC2 Amazon-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben](#)
- [\[SSM.4\] SSM-Dokumente sollten nicht öffentlich sein](#)
- [\[WAF.2\] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.3\] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.4\] AWS WAF Classic Regional Web ACLs sollte mindestens eine Regel oder Regelgruppe enthalten](#)
- [\[WAF.10\] AWS WAF web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)

Weitere Informationen zu diesem Standard finden Sie unter [Security Hub CSPM-Steuerelemente](#) im AWS Control Tower Benutzerhandbuch.

Einen Sicherheitsstandard aktivieren

Wenn Sie einen Sicherheitsstandard in Security Hub Cloud AWS Security Posture Management (CSPM) aktivieren, erstellt und aktiviert Security Hub CSPM automatisch alle Kontrollen, die für den Standard gelten. Security Hub CSPM beginnt auch mit der Durchführung von Sicherheitsprüfungen und der Generierung von Ergebnissen für die Kontrollen.

Um die Abdeckung und Genauigkeit der Ergebnisse zu optimieren, aktivieren und konfigurieren Sie die Ressourcenaufzeichnung, AWS Config bevor Sie einen Standard aktivieren. Achten Sie bei der Konfiguration der Ressourcenaufzeichnung auch darauf, sie für alle Ressourcentypen zu aktivieren, die durch die für den Standard geltenden Kontrollen überprüft werden. Andernfalls ist Security Hub CSPM möglicherweise nicht in der Lage, die geeigneten Ressourcen zu bewerten und genaue Ergebnisse für Kontrollen zu generieren, die für den Standard gelten. Weitere Informationen finden Sie unter [Aktivierung und Konfiguration AWS Config für Security Hub CSPM](#).

Nachdem Sie einen Standard aktiviert haben, können Sie einzelne Kontrollen, die für den Standard gelten, deaktivieren oder später wieder aktivieren. Wenn Sie ein Steuerelement für einen Standard deaktivieren, generiert Security Hub CSPM keine Ergebnisse mehr für das Steuerelement. Darüber hinaus ignoriert Security Hub CSPM das Steuerelement bei der Berechnung der Sicherheitsbewertung für den Standard. Die Sicherheitsbewertung ist der Prozentsatz der Kontrollen, die die Bewertung bestanden haben, im Verhältnis zur Gesamtzahl der Kontrollen, die für den Standard gelten, aktiviert sind und über Bewertungsdaten verfügen.

Wenn Sie einen Standard aktivieren, generiert Security Hub CSPM eine vorläufige Sicherheitsbewertung für den Standard, in der Regel innerhalb von 30 Minuten nach Ihrem ersten Besuch der Seite Zusammenfassung oder Sicherheitsstandards auf der Security Hub CSPM-Konsole. Sicherheitsbewertungen werden nur für Standards generiert, die aktiviert sind, wenn Sie diese Seiten auf der Konsole aufrufen. Darüber hinaus muss die Ressourcenaufzeichnung konfiguriert sein, damit AWS Config die Punktzahlen angezeigt werden. In den China Regionen und kann es bis zu 24 Stunden dauern AWS GovCloud (US) Regions, bis Security Hub CSPM eine vorläufige Sicherheitsbewertung für einen Standard generiert. Nachdem Security Hub CSPM eine vorläufige Bewertung generiert hat, wird die Bewertung alle 24 Stunden aktualisiert. Um festzustellen, wann eine Sicherheitsbewertung zuletzt aktualisiert wurde, können Sie sich auf einen Zeitstempel beziehen, den Security Hub CSPM für die Bewertung bereitstellt. Weitere Informationen finden Sie unter [Berechnung von Sicherheitswerten](#).

Wie Sie einen Standard aktivieren, hängt davon ab, ob Sie die [zentrale Konfiguration](#) verwenden, um Security Hub CSPM für mehrere Konten zu verwalten und. AWS-Regionen Wir empfehlen die zentrale Konfiguration, wenn Sie Standards in Umgebungen mit mehreren Konten und mehreren Regionen aktivieren möchten. Sie können die zentrale Konfiguration verwenden, wenn Sie Security Hub CSPM mit integrieren. AWS Organizations Wenn Sie die zentrale Konfiguration nicht verwenden, müssen Sie jeden Standard separat in jedem Konto und jeder Region aktivieren.

Themen

- [Aktivierung eines Standards in mehreren Konten und AWS-Regionen](#)
- [Aktivierung eines Standards in einem einzigen Konto und AWS-Region](#)
- [Den Status eines Standards überprüfen](#)

Aktivierung eines Standards in mehreren Konten und AWS-Regionen

Verwenden Sie die [zentrale Konfiguration, um einen Sicherheitsstandard für mehrere Konten zu aktivieren und AWS-Regionen zu konfigurieren](#). Bei der zentralen Konfiguration kann der

delegierte Security Hub CSPM-Administrator Security Hub CSPM-Konfigurationsrichtlinien erstellen, die einen oder mehrere Standards aktivieren. Der Administrator kann dann einzelnen Konten, Organisationseinheiten (OUs) oder dem Stammkonto eine Konfigurationsrichtlinie zuordnen. Eine Konfigurationsrichtlinie wirkt sich auf die Heimatregion, die auch als Aggregationsregion bezeichnet wird, und auf alle verknüpften Regionen aus.

Konfigurationsrichtlinien bieten Anpassungsoptionen. Sie können sich beispielsweise dafür entscheiden, nur den FSBP-Standard (AWS Foundational Security Best Practices) für eine Organisationseinheit zu aktivieren. Für eine andere Organisationseinheit könnten Sie sich dafür entscheiden, sowohl den FSBP-Standard als auch den Benchmark v1.4.0-Standard der Center for Internet Security (CIS) AWS Foundations zu aktivieren. Informationen zum Erstellen einer Konfigurationsrichtlinie, die bestimmte von Ihnen angegebene Standards aktiviert, finden Sie unter [Konfigurationsrichtlinien erstellen und zuordnen](#)

Wenn Sie die zentrale Konfiguration verwenden, aktiviert Security Hub CSPM nicht automatisch Standards in neuen oder bestehenden Konten. Stattdessen gibt der Security Hub CSPM-Administrator an, welche Standards für verschiedene Konten aktiviert werden sollen, wenn er Security Hub CSPM-Konfigurationsrichtlinien für seine Organisation erstellt. Security Hub CSPM bietet eine empfohlene Konfigurationsrichtlinie, in der nur der FSBP-Standard aktiviert ist. Weitere Informationen finden Sie unter [Arten von Konfigurationsrichtlinien](#).

Note

Der Security Hub CSPM-Administrator kann mithilfe von Konfigurationsrichtlinien jeden Standard außer dem vom [AWS Control Tower Service](#) verwalteten Standard aktivieren. Um diesen Standard zu aktivieren, muss der Administrator ihn direkt verwenden. AWS Control Tower Sie müssen außerdem einzelne Steuerungen in diesem Standard für ein zentral verwaltetes Konto aktivieren oder deaktivieren. AWS Control Tower

Wenn Sie möchten, dass einige Konten Standards für ihre eigenen Konten aktivieren und konfigurieren, kann der Security Hub CSPM-Administrator diese Konten als selbstverwaltete Konten kennzeichnen. Selbstverwaltete Konten müssen Standards in jeder Region separat aktivieren und konfigurieren.

Aktivierung eines Standards in einem einzigen Konto und AWS-Region

Wenn Sie keine zentrale Konfiguration verwenden oder über ein selbstveraltetes Konto verfügen, können Sie keine Konfigurationsrichtlinien verwenden, um Sicherheitsstandards zentral in mehreren

Konten zu aktivieren oder AWS-Regionen. Sie können jedoch einen Standard für ein einzelnes Konto und eine Region aktivieren. Sie können dies mithilfe der Security Hub CSPM-Konsole oder der Security Hub CSPM-API tun.

Security Hub CSPM console

Gehen Sie wie folgt vor, um mithilfe der Security Hub CSPM-Konsole einen Standard für ein Konto und eine Region zu aktivieren.

Um einen Standard in einem Konto und einer Region zu aktivieren

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie den Standard aktivieren möchten.
3. Wählen Sie im Navigationsbereich die Option Sicherheitsstandards aus. Auf der Seite Sicherheitsstandards sind alle Standards aufgeführt, die Security Hub CSPM derzeit unterstützt. Wenn Sie bereits einen Standard aktiviert haben, enthält der Abschnitt für den Standard die aktuelle Sicherheitsbewertung und zusätzliche Details zum Standard.
4. Wählen Sie im Abschnitt für den Standard, den Sie aktivieren möchten, die Option Standard aktivieren aus.

Um den Standard in weiteren Regionen zu aktivieren, wiederholen Sie die vorherigen Schritte in jeder weiteren Region.

Security Hub CSPM API

Verwenden Sie den Vorgang, um einen Standard programmgesteuert in einem einzigen Konto und einer Region zu aktivieren. [BatchEnableStandards](#) Oder, wenn Sie die AWS Command Line Interface (AWS CLI) verwenden, führen Sie den [batch-enable-standards](#) Befehl aus.

Verwenden Sie in Ihrer Anfrage den `StandardsArn` Parameter, um den Amazon-Ressourcennamen (ARN) des Standards anzugeben, den Sie aktivieren möchten. Geben Sie auch die Region an, für die Ihre Anfrage gilt. Mit dem folgenden Befehl wird beispielsweise der FSBP-Standard (AWS Foundational Security Best Practices) aktiviert:

```
$ aws securityhub batch-enable-standards \
--standards-subscription-requests '{"StandardsArn":"arn:aws:securityhub:us-
east-1::standards/aws-foundational-security-best-practices/v/1.0.0"}' \
```

```
--region us-east-1
```

Wo *arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0* ist der ARN des FSBP-Standards in der Region USA Ost (Nord-Virginia), und *us-east-1* ist die Region, in der er aktiviert werden soll.

Um den ARN für einen Standard abzurufen, verwenden Sie den [DescribeStandards](#)Vorgang oder, falls Sie den verwenden AWS CLI, führen Sie den [describe-standards](#)Befehl aus.

Um zunächst eine Liste der Standards zu überprüfen, die derzeit in Ihrem Konto aktiviert sind, können Sie den [GetEnabledStandards](#)Vorgang verwenden. Wenn Sie den verwenden AWS CLI, können Sie den [get-enabled-standards](#)Befehl ausführen, um diese Liste abzurufen.

Nachdem Sie einen Standard aktiviert haben, beginnt Security Hub CSPM mit der Ausführung von Aufgaben, um den Standard im Konto und in der angegebenen Region zu aktivieren. Dazu gehört die Erstellung aller Kontrollen, die für den Standard gelten. Um den Status dieser Aufgaben zu überwachen, können Sie den Status des Standards für das Konto und die Region überprüfen.

Den Status eines Standards überprüfen

Wenn Sie einen Sicherheitsstandard für ein Konto aktivieren, beginnt Security Hub CSPM mit der Erstellung aller Kontrollen, die für den Standard im Konto gelten. Security Hub CSPM führt auch zusätzliche Aufgaben aus, um den Standard für das Konto zu aktivieren, z. B. die Generierung einer vorläufigen Sicherheitsbewertung für den Standard. Während Security Hub CSPM diese Aufgaben ausführt, bezieht sich der Status des Standards auf das PendingKonto. Der Status des Standards durchläuft dann weitere Status, die Sie überwachen und überprüfen können.

Note

Änderungen an einzelnen Kontrollen für eine Norm wirken sich nicht auf den Gesamtstatus der Norm aus. Wenn Sie beispielsweise ein Steuerelement aktivieren, das Sie zuvor deaktiviert haben, wirkt sich Ihre Änderung nicht auf den Status des Standards aus. Ebenso wirkt sich Ihre Änderung nicht auf den Status des Standards aus, wenn Sie einen Parameterwert für ein aktiviertes Steuerelement ändern.

Um den Status eines Standards mithilfe der Security Hub CSPM-Konsole zu überprüfen, wählen Sie im Navigationsbereich Sicherheitsstandards aus. Auf der Seite Sicherheitsstandards sind alle

Standards aufgeführt, die Security Hub CSPM derzeit unterstützt. Wenn Security Hub CSPM derzeit Aufgaben zur Aktivierung des Standards ausführt, gibt der Abschnitt für den Standard an, dass Security Hub CSPM immer noch eine Sicherheitsbewertung für den Standard generiert. Wenn ein Standard aktiviert ist, enthält der Abschnitt für den Standard die aktuelle Bewertung. Wählen Sie Ergebnisse anzeigen, um zusätzliche Details zu überprüfen, einschließlich des Status einzelner Kontrollen, die für den Standard gelten. Weitere Informationen finden Sie unter [Zeitplan für die Ausführung von Sicherheitsprüfungen](#).

Verwenden Sie den Vorgang, um den Status eines Standards programmgesteuert mit der Security Hub CSPM-API zu überprüfen. [GetEnabledStandards](#) Verwenden Sie in Ihrer Anfrage optional den `StandardsSubscriptionArns` Parameter, um den Amazon-Ressourcennamen (ARN) des Standards anzugeben, dessen Status Sie überprüfen möchten. Wenn Sie AWS Command Line Interface (AWS CLI) verwenden, können Sie den [get-enabled-standards](#) Befehl ausführen, um den Status eines Standards zu überprüfen. Verwenden Sie den `standards-subscription-arns` Parameter, um den ARN des zu prüfenden Standards anzugeben. Um zu ermitteln, welcher ARN angegeben werden soll, können Sie den [DescribeStandards](#) Vorgang verwenden oder für den den AWS CLI den [describe-standards](#) Befehl ausführen.

Wenn Ihre Anfrage erfolgreich ist, antwortet Security Hub CSPM mit einer Reihe von Objekten. **StandardsSubscription** Ein Standardabonnement ist eine AWS Ressource, die Security Hub CSPM in einem Konto erstellt, wenn ein Standard für das Konto aktiviert ist. Jedes **StandardsSubscription** Objekt enthält Details zu einem Standard, der derzeit für das Konto aktiviert ist oder gerade aktiviert oder deaktiviert wird. In jedem Objekt gibt das **StandardsStatus** Feld den aktuellen Status des Standards für das Konto an.

Der Status eines Standards (**StandardsStatus**) kann einer der folgenden sein.

PENDING

Security Hub CSPM führt derzeit Aufgaben aus, um den Standard für das Konto zu aktivieren. Dazu gehören die Erstellung der Kontrollen, die für den Standard gelten, und die Erstellung einer vorläufigen Sicherheitsbewertung für den Standard. Es kann mehrere Minuten dauern, bis Security Hub CSPM alle Aufgaben abgeschlossen hat. Ein Standard kann diesen Status auch haben, wenn er bereits für das Konto aktiviert ist und Security Hub CSPM dem Standard derzeit neue Steuerungen hinzufügt.

Wenn ein Standard diesen Status hat, können Sie möglicherweise nicht die Details einzelner Kontrollen abrufen, die für den Standard gelten. Darüber hinaus sind Sie möglicherweise nicht in der Lage, einzelne Steuerelemente für den Standard zu konfigurieren oder zu deaktivieren. Wenn

Sie beispielsweise versuchen, ein Steuerelement mithilfe des [UpdateStandardsControl](#)Vorgangs zu deaktivieren, tritt ein Fehler auf.

Anhand des Werts für das `StandardsControlsUpdatable` Feld können Sie feststellen, ob Sie einzelne Steuerelemente für den Standard konfigurieren oder anderweitig verwalten können. Wenn der Wert für dieses Feld lautet `READY_FOR_UPDATES`, können Sie mit der Verwaltung einzelner Steuerelemente für den Standard beginnen. Warten Sie andernfalls, bis Security Hub CSPM zusätzliche Verarbeitungsaufgaben abgeschlossen hat, um den Standard zu aktivieren.

READY

Der Standard ist derzeit für das Konto aktiviert. Security Hub CSPM kann Sicherheitsprüfungen durchführen und Ergebnisse für alle Kontrollen generieren, die für den Standard gelten und derzeit aktiviert sind. Security Hub CSPM kann auch eine Sicherheitsbewertung für den Standard berechnen.

Wenn ein Standard diesen Status hat, können Sie die Details einzelner Kontrollen abrufen, die für den Standard gelten. Darüber hinaus können Sie die Steuerelemente konfigurieren, deaktivieren oder erneut aktivieren. Sie können den Standard auch deaktivieren.

INCOMPLETE

Security Hub CSPM konnte den Standard für das Konto nicht vollständig aktivieren. Security Hub CSPM kann keine Sicherheitsprüfungen durchführen und keine Ergebnisse für alle Kontrollen generieren, die für den Standard gelten und derzeit aktiviert sind. Darüber hinaus kann Security Hub CSPM keine Sicherheitsbewertung für den Standard berechnen.

Anhand der Informationen im Array können Sie feststellen, warum der Standard nicht vollständig aktiviert wurde. `StandardsStatusReason` Dieses Array spezifiziert Probleme, die Security Hub CSPM daran gehindert haben, den Standard zu aktivieren. Wenn ein interner Fehler aufgetreten ist, versuchen Sie erneut, den Standard für das Konto zu aktivieren. Bei anderen Problemen [überprüfen Sie Ihre AWS Config Einstellungen](#). Sie können auch [einzelne Steuerelemente deaktivieren](#), die Sie nicht überprüfen möchten, oder den Standard vollständig deaktivieren.

DELETING

Security Hub CSPM bearbeitet derzeit eine Anfrage zur Deaktivierung des Standards für das Konto. Dazu gehören die Deaktivierung der Kontrollen, die für den Standard gelten, und das Entfernen der zugehörigen Sicherheitsbewertung. Es kann mehrere Minuten dauern, bis Security Hub CSPM die Bearbeitung der Anfrage abgeschlossen hat.

Wenn ein Standard diesen Status hat, können Sie den Standard nicht erneut aktivieren oder erneut versuchen, ihn für das Konto zu deaktivieren. Security Hub CSPM muss zuerst die Bearbeitung der aktuellen Anfrage abschließen. Darüber hinaus können Sie die Details einzelner Kontrollen, die für den Standard gelten, nicht abrufen oder die Kontrollen verwalten.

FAILED

Security Hub CSPM konnte den Standard für das Konto nicht deaktivieren. Ein oder mehrere Fehler traten auf, als Security Hub CSPM versuchte, den Standard zu deaktivieren. Darüber hinaus kann Security Hub CSPM keine Sicherheitsbewertung für den Standard berechnen.

Anhand der Informationen im Array können Sie feststellen, warum der Standard nicht vollständig deaktiviert wurde. `StandardsStatusReason` Dieses Array spezifiziert Probleme, die Security Hub CSPM daran gehindert haben, den Standard zu deaktivieren.

Wenn ein Standard diesen Status hat, können Sie die Details einzelner Kontrollen, die für den Standard gelten, nicht abrufen oder die Kontrollen verwalten. Sie können den Standard jedoch für das Konto wieder aktivieren. Wenn Sie die Probleme beheben, die Security Hub CSPM daran gehindert haben, den Standard zu deaktivieren, können Sie auch erneut versuchen, den Standard zu deaktivieren.

Wenn der Status eines Standards lautet `READY`, führt Security Hub CSPM Sicherheitsprüfungen durch und generiert Ergebnisse für alle Kontrollen, die für den Standard gelten und derzeit aktiviert sind. Bei anderen Status führt Security Hub CSPM möglicherweise Prüfungen durch und generiert Ergebnisse für einige, aber nicht alle aktivierten Kontrollen. Es kann bis zu 24 Stunden dauern, bis die Kontrollergebnisse generiert oder aktualisiert werden. Weitere Informationen finden Sie unter [Zeitplan für die Ausführung von Sicherheitsprüfungen](#).

Überprüfung der Einzelheiten eines Sicherheitsstandards

Nachdem Sie einen Sicherheitsstandard in Security Hub Cloud AWS Security Posture Management (CSPM) aktiviert haben, können Sie die Konsole verwenden, um die Details des Standards zu überprüfen. Auf der Konsole enthält die Detailseite für einen Standard die folgenden Informationen:

- Die aktuelle Sicherheitsbewertung für den Standard.
- Eine Tabelle mit Kontrollen, die für den Standard gelten.
- Aggregierte Statistiken für Kontrollen, die für den Standard gelten.
- Eine visuelle Zusammenfassung des Status der Kontrollen, die für den Standard gelten.

- Eine visuelle Zusammenfassung der Sicherheitsprüfungen für Kontrollen, die aktiviert sind und dem Standard entsprechen. Bei der Integration mit gelten Steuerelemente AWS Organizations, die in mindestens einem Organisationskonto aktiviert sind, als aktiviert.

Um diese Details zu überprüfen, wählen Sie im Navigationsbereich der Konsole Sicherheitsstandards aus. Wählen Sie dann im Abschnitt für den Standard die Option Ergebnisse anzeigen aus. Für eine eingehendere Analyse können Sie die Daten filtern und sortieren und sich die Details der einzelnen Kontrollen ansehen, die für den Standard gelten.

Themen

- [Grundlegendes zur Standard-Sicherheitsbewertung](#)
- [Überprüfung der Kontrollen im Hinblick auf einen Standard](#)

Grundlegendes zur Standard-Sicherheitsbewertung

Auf der AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole wird auf der Detailseite für einen Standard die Sicherheitsbewertung für den Standard angezeigt. Die Punktzahl ist der Prozentsatz der Kontrollen, die die Bewertung bestanden haben, im Verhältnis zur Gesamtzahl der Kontrollen, die für den Standard gelten, aktiviert sind und über Bewertungsdaten verfügen. Unter der Punktzahl befindet sich ein Diagramm, das die Sicherheitsüberprüfungen für Kontrollen zusammenfasst, die für den Standard aktiviert sind. Dies beinhaltet die Anzahl der bestanden und fehlgeschlagenen Sicherheitsprüfungen. Bei Administratorkonten werden die Standardpunktzahl und das Diagramm für das Administratorkonto und alle Mitgliedskonten zusammengefasst. Um fehlgeschlagene Sicherheitsüberprüfungen auf Kontrollen mit einem bestimmten Schweregrad zu überprüfen, wählen Sie den Schweregrad aus.

Wenn Sie einen Standard aktivieren, generiert Security Hub CSPM eine vorläufige Sicherheitsbewertung für den Standard, in der Regel innerhalb von 30 Minuten nach Ihrem ersten Besuch der Übersichtsseite oder der Seite Sicherheitsstandards auf der Security Hub CSPM-Konsole. Bewertungen werden nur für Standards generiert, die aktiviert sind, wenn Sie diese Seiten besuchen. Darüber hinaus muss die AWS Config Ressourcenaufzeichnung konfiguriert werden, damit die Ergebnisse angezeigt werden. In den Regionen China und kann es bis zu 24 Stunden dauern AWS GovCloud (US) Regions, bis Security Hub CSPM eine vorläufige Bewertung generiert. Nachdem Security Hub CSPM eine vorläufige Bewertung für einen Standard generiert hat, wird die Bewertung alle 24 Stunden aktualisiert. Weitere Informationen finden Sie unter [Berechnung von Sicherheitswerten](#).

Alle Daten auf den Detailseiten zu Sicherheitsstandards beziehen sich auf den aktuellen Stand, AWS-Region sofern Sie keine Aggregationsregion festlegen. Wenn Sie eine Aggregationsregion festlegen, gelten die Sicherheitsbewertungen für alle Regionen und beinhalten Ergebnisse für alle verknüpften Regionen. Darüber hinaus spiegelt der Konformitätsstatus der Kontrollen Ergebnisse aus verknüpften Regionen wider, und die Anzahl der Sicherheitsprüfungen umfasst Ergebnisse aus verknüpften Regionen.

Überprüfung der Kontrollen im Hinblick auf einen Standard

Wenn Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole verwenden, um die Details eines von Ihnen aktivierten Standards zu überprüfen, können Sie sich eine Tabelle mit Sicherheitskontrollen ansehen, die für den Standard gelten. Die Tabelle enthält für jedes Steuerelement die folgenden Informationen:

- Die Kontroll-ID und der Titel.
- Der Status des Steuerelements. Weitere Informationen finden Sie unter [Bewertung des Konformitätsstatus und des Kontrollstatus](#).
- Der Schweregrad, der der Kontrolle zugewiesen wurde.
- Die Anzahl der fehlgeschlagenen Prüfungen und die Gesamtzahl der Prüfungen. Falls zutreffend, gibt das Feld Fehlgeschlagene Prüfungen auch die Anzahl der Ergebnisse mit dem Status Unbekannt an.
- Ob das Steuerelement benutzerdefinierte Parameter unterstützt. Weitere Informationen finden Sie unter [Grundlegendes zu den Steuerparametern in Security Hub CSPM](#).

Security Hub CSPM-Updates kontrollieren den Status und die Anzahl der Sicherheitschecks alle 24 Stunden. Ein Zeitstempel oben auf der Seite gibt an, wann Security Hub CSPM diese Daten zuletzt aktualisiert hat.

Bei Administratorkonten werden der Kontrollstatus und die Anzahl der Sicherheitsüberprüfungen für das Administratorkonto und alle Mitgliedskonten zusammengefasst. Die Anzahl der aktivierten Kontrollen umfasst Kontrollen, die standardmäßig im Administratorkonto oder in mindestens einem Mitgliedskonto aktiviert sind. Die Anzahl der deaktivierten Steuerelemente umfasst Steuerelemente, die standardmäßig im Administratorkonto und in allen Mitgliedskonten deaktiviert sind.

Sie können die Tabelle mit den Steuerelementen filtern, die für den Standard gelten. Mithilfe der Optionen „Nach filtern“ neben der Tabelle können Sie wählen, ob nur aktivierte oder nur deaktivierte Steuerelemente für den Standard angezeigt werden sollen. Wenn Sie nur aktivierte Steuerelemente

anzeigen, können Sie die Tabelle weiter nach dem Status der Steuerelemente filtern. Sie können sich dann auf Steuerelemente konzentrieren, die einen bestimmten Kontrollstatus haben. Zusätzlich zu den Optionen Filtern nach können Sie Filterkriterien in das Feld Steuerelemente filtern eingeben. Sie können beispielsweise nach der Kontroll-ID oder dem Titel filtern.

Wählen Sie Ihre bevorzugte Zugriffsmethode. Folgen Sie dann den Schritten, um die Kontrollen zu überprüfen, die für einen von Ihnen aktivierten Standard gelten.

Security Hub CSPM console

Um die Steuerelemente für einen aktivierten Standard zu überprüfen

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Sicherheitsstandards aus.
3. Wählen Sie im Abschnitt für den Standard die Option Ergebnisse anzeigen aus.

In der Tabelle unten auf der Seite sind alle Steuerelemente aufgeführt, die für den Standard gelten. Sie können die Tabelle filtern und sortieren. Sie können die aktuelle Seite der Tabelle auch als CSV-Datei herunterladen. Wählen Sie dazu oberhalb der Tabelle die Option Herunterladen aus. Wenn Sie die Tabelle filtern, enthält die heruntergeladene Datei nur die Steuerelemente, die Ihren aktuellen Filtereinstellungen entsprechen.

Security Hub CSPM API

Um die Steuerelemente für einen aktivierten Standard zu überprüfen

1. Verwenden Sie den [ListSecurityControlDefinitions](#)Betrieb der Security Hub CSPM-API. Wenn Sie den verwenden AWS CLI, führen Sie den [list-security-control-definitions](#)Befehl aus.

Geben Sie den Amazon-Ressourcennamen (ARN) des Standards an, für den Sie die Kontrollen überprüfen möchten. Um nach Standards zu ARNs suchen, verwenden Sie den [DescribeStandards](#)Vorgang oder führen Sie den Befehl [describe-standards](#) aus. Wenn Sie den ARN für einen Standard nicht angeben, gibt Security Hub CSPM die gesamte Sicherheitskontrolle zurück. IDs

2. Verwenden Sie den [ListStandardsControlAssociations](#)Betrieb der Security Hub CSPM-API oder führen Sie den [list-standards-control-associations](#)Befehl aus. Dieser Vorgang gibt an, in welchen Standards ein Steuerelement aktiviert ist.

Identifizieren Sie das Steuerelement, indem Sie die Sicherheitskontroll-ID oder den ARN angeben. Paginierungsparameter sind optional.

Das folgende Beispiel zeigt Ihnen, in welchen Standards das Config.1-Steuerelement aktiviert ist.

```
$ aws securityhub list-standards-control-associations --region us-east-1 --security-control-id Config.1
```

Durch das Ausschalten automatisch aktivierter Sicherheitsstandards

Wenn Ihre Organisation keine zentrale Konfiguration verwendet, verwendet sie einen Konfigurationstyp, der als lokale Konfiguration bezeichnet wird. Mit der lokalen Konfiguration kann AWS Security Hub Cloud Security Posture Management (CSPM) automatisch Standardsicherheitsstandards für neue Mitgliedskonten aktivieren, wenn die Konten Ihrer Organisation beitreten. Alle Kontrollen, die für diese Standardstandards gelten, werden ebenfalls automatisch aktiviert.

Derzeit sind die Standardsicherheitsstandards der Standard AWS Foundational Security Best Practices und der Benchmark v1.2.0-Standard der Center for Internet Security (CIS) AWS Foundations. Informationen zu diesen Standards finden Sie im [Standardreferenz für Security Hub CSPM](#)

Wenn Sie Sicherheitsstandards für neue Mitgliedskonten lieber manuell aktivieren möchten, können Sie die automatische Aktivierung der Standardstandards deaktivieren. Dies ist nur möglich, wenn Sie die lokale Konfiguration integrieren AWS Organizations und diese verwenden. Wenn Sie die zentrale Konfiguration verwenden, können Sie stattdessen eine Konfigurationsrichtlinie erstellen, die die Standardstandards aktiviert, und die Richtlinie dem Stammverzeichnis zuordnen. Alle Ihre Unternehmenskonten und erben OUs dann diese Konfigurationsrichtlinie, sofern sie nicht mit einer anderen Richtlinie verknüpft sind oder selbst verwaltet werden. Wenn Sie nicht integrieren AWS Organizations, können Sie einen Standardstandard deaktivieren, wenn Sie Security Hub CSPM zum ersten Mal oder später aktivieren. Um zu erfahren wie dies geht, vgl. [Deaktivierung eines Standards](#).

Um die automatische Aktivierung der Standardstandards für neue Mitgliedskonten zu deaktivieren, können Sie die Security Hub CSPM-Konsole oder die Security Hub CSPM-API verwenden.

Security Hub CSPM console

Gehen Sie wie folgt vor, um die automatische Aktivierung der Standardstandards mithilfe der Security Hub CSPM-Konsole zu deaktivieren.

Um die automatische Aktivierung von Standardstandards zu deaktivieren

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>

Melden Sie sich mit den Anmeldeinformationen des Administratorkontos an.

2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Konfiguration aus.
3. Wählen Sie im Abschnitt Übersicht die Option Bearbeiten aus.
4. Deaktivieren Sie unter Neue Kontoeinstellungen das Kontrollkästchen Standardsicherheitsstandards aktivieren.
5. Wählen Sie Bestätigen aus.

Security Hub CSPM API

Um die automatische Aktivierung der Standardstandards programmgesteuert zu deaktivieren, verwenden Sie vom Security Hub CSPM-Administratorkonto aus den [UpdateOrganizationConfiguration](#) Betrieb der Security Hub CSPM-API. Geben Sie in Ihrer Anfrage den Parameter an. `NONE AutoEnableStandards`

Wenn Sie den verwenden AWS CLI, führen Sie den [update-organization-configuration](#) Befehl aus, um die automatische Aktivierung der Standardstandards zu deaktivieren. Geben Sie für den Parameter `auto-enable-standards` `NONE` an: Der folgende Befehl aktiviert beispielsweise automatisch Security Hub CSPM für neue Mitgliedskonten und deaktiviert die automatische Aktivierung der Standardstandards für die Konten.

```
$ aws securityhub update-organization-configuration --auto-enable --auto-enable-standards NONE
```

Deaktivierung eines Sicherheitsstandards

Wenn Sie einen Sicherheitsstandard in Security Hub Cloud AWS Security Posture Management (CSPM) deaktivieren, passiert Folgendes:

- Alle Kontrollen, die für den Standard gelten, sind deaktiviert, sofern sie nicht mit einem anderen Standard verknüpft sind, der derzeit aktiviert ist.
- Sicherheitsprüfungen für die deaktivierten Steuerelemente werden nicht mehr durchgeführt, und es werden keine weiteren Ergebnisse für die deaktivierten Steuerelemente generiert.
- Bestehende Ergebnisse für die deaktivierten Kontrollen werden nach etwa 3-5 Tagen automatisch archiviert.
- AWS Config Regeln, die Security Hub CSPM für die deaktivierten Steuerelemente erstellt hat, werden gelöscht.

Das Löschen der entsprechenden AWS Config Regeln erfolgt in der Regel innerhalb weniger Minuten nach der Deaktivierung eines Standards. Es kann jedoch länger dauern. Wenn die erste Anfrage die Regeln nicht löscht, versucht Security Hub CSPM alle 12 Stunden erneut. Wenn Sie Security Hub CSPM jedoch deaktiviert haben oder keine anderen Standards aktiviert haben, kann Security Hub CSPM es nicht erneut versuchen, was bedeutet, dass die Regeln nicht gelöscht werden können. Wenn dies der Fall ist und Sie die Regeln löschen müssen, wenden Sie sich an AWS -Support

Themen

- [Deaktivierung eines Standards in mehreren Konten und AWS-Regionen](#)
- [Deaktivierung eines Standards in einem einzelnen Konto und AWS-Region](#)

Deaktivierung eines Standards in mehreren Konten und AWS-Regionen

Verwenden Sie die [zentrale Konfiguration AWS-Regionen](#), um einen Sicherheitsstandard für mehrere Konten und zu deaktivieren. Bei der zentralen Konfiguration kann der delegierte Security Hub CSPM-Administrator Security Hub CSPM-Konfigurationsrichtlinien erstellen, die einen oder mehrere Standards deaktivieren. Der Administrator kann dann einzelnen Konten, Organisationseinheiten (OUs) oder dem Stammkonto eine Konfigurationsrichtlinie zuordnen. Eine Konfigurationsrichtlinie wirkt sich auf die Heimatregion, die auch als Aggregationsregion bezeichnet wird, und auf alle verknüpften Regionen aus.

Konfigurationsrichtlinien bieten Anpassungsoptionen. Sie könnten sich beispielsweise dafür entscheiden, den Payment Card Industry Data Security Standard (PCI DSS) in einer Organisationseinheit zu deaktivieren. Für eine andere Organisationseinheit könnten Sie sich dafür entscheiden, sowohl den PCI DSS als auch den Standard SP 800-53 Rev. 5 des National Institute of Standards and Technology (NIST) zu deaktivieren. Informationen zum Erstellen einer

Konfigurationsrichtlinie, die einzelne von Ihnen angegebene Standards aktiviert oder deaktiviert, finden Sie unter. [Konfigurationsrichtlinien erstellen und zuordnen](#)

 Note

Der Security Hub CSPM-Administrator kann mithilfe von Konfigurationsrichtlinien jeden Standard außer dem vom [AWS Control Tower Service](#) verwalteten Standard deaktivieren. Um diesen Standard zu deaktivieren, muss der Administrator ihn direkt verwenden. AWS Control Tower Sie müssen außerdem einzelne Steuerungen in diesem Standard für ein zentral verwaltetes Konto verwenden, AWS Control Tower um sie zu deaktivieren oder zu aktivieren.

Wenn Sie möchten, dass einige Konten Standards für ihre eigenen Konten konfigurieren oder deaktivieren, kann der Security Hub CSPM-Administrator diese Konten als selbstverwaltete Konten kennzeichnen. Selbstverwaltete Konten müssen die Standards in jeder Region separat deaktivieren.

Deaktivierung eines Standards in einem einzelnen Konto und AWS-Region

Wenn Sie die zentrale Konfiguration nicht verwenden oder über ein selbstveraltetes Konto verfügen, können Sie keine Konfigurationsrichtlinien verwenden, um Sicherheitsstandards in mehreren Konten zentral zu deaktivieren oder. AWS-Regionen Sie können jedoch einen Standard für ein einzelnes Konto und eine Region deaktivieren. Sie können dies mithilfe der Security Hub CSPM-Konsole oder der Security Hub CSPM-API tun.

Security Hub CSPM console

Gehen Sie wie folgt vor, um einen Standard in einem Konto und einer Region mithilfe der Security Hub CSPM-Konsole zu deaktivieren.

Um einen Standard in einem Konto und einer Region zu deaktivieren

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie mithilfe der AWS-Region Auswahl Taste in der oberen rechten Ecke der Seite die Region aus, in der Sie den Standard deaktivieren möchten.
3. Wählen Sie im Navigationsbereich die Option Sicherheitsstandards aus.
4. Wählen Sie im Abschnitt für den Standard, den Sie deaktivieren möchten, die Option Standard deaktivieren aus.

Um den Standard in weiteren Regionen zu deaktivieren, wiederholen Sie die vorherigen Schritte in jeder weiteren Region.

Security Hub CSPM API

Verwenden Sie den Vorgang, um einen Standard programmgesteuert in einem einzelnen Konto und einer Region zu deaktivieren. [BatchDisableStandards](#) Oder, wenn Sie die AWS Command Line Interface (AWS CLI) verwenden, führen Sie den [batch-disable-standards](#) Befehl aus.

Verwenden Sie in Ihrer Anfrage den `StandardsSubscriptionArns` Parameter, um den Amazon-Ressourcennamen (ARN) des Standards anzugeben, den Sie deaktivieren möchten. Wenn Sie den verwenden AWS CLI, verwenden Sie den `standards-subscription-arns` Parameter, um den ARN anzugeben. Geben Sie auch die Region an, für die sich Ihre Anfrage bezieht. Der folgende Befehl deaktiviert beispielsweise den FSBP-Standard (AWS Foundational Security Best Practices) für ein Konto (): **123456789012**

```
$ aws securityhub batch-disable-standards \
--standards-subscription-arns "arn:aws:securityhub:us-east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0" \
--region us-east-1
```

Wo **arn:aws:securityhub:us-east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0** ist der ARN des FSBP-Standards für das Konto in der Region USA Ost (Nord-Virginia), und **us-east-1** ist die Region, in der es deaktiviert werden soll.

Um den ARN für einen Standard zu erhalten, können Sie die [GetEnabledStandards](#) Operation verwenden. Bei diesem Vorgang werden Informationen zu den Standards abgerufen, die derzeit in Ihrem Konto aktiviert sind. Wenn Sie den verwenden AWS CLI, können Sie den [get-enabled-standards](#) Befehl ausführen, um diese Informationen abzurufen.

Nachdem Sie einen Standard deaktiviert haben, beginnt Security Hub CSPM mit der Ausführung von Aufgaben zur Deaktivierung des Standards im Konto und in der angegebenen Region. Dazu gehört auch die Deaktivierung aller Kontrollen, die für den Standard gelten. Um den Status dieser Aufgaben zu überwachen, können Sie [den Status des Standards für das](#) Konto und die Region überprüfen.

Grundlegendes zu den Sicherheitskontrollen in Security Hub CSPM

In AWS Security Hub Cloud Security Posture Management (CSPM) ist eine Sicherheitskontrolle, auch als Kontrolle bezeichnet, eine Schutzmaßnahme innerhalb eines Sicherheitsstandards, die einem Unternehmen hilft, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationen zu schützen. In Security Hub CSPM bezieht sich ein Steuerelement auf eine bestimmte AWS Ressource.

Wenn Sie ein Steuerelement in einem oder mehreren Standards aktivieren, beginnt Security Hub CSPM mit der Durchführung von Sicherheitsüberprüfungen. Die Sicherheitsüberprüfungen führen zu Ergebnissen des Security Hub CSPM. Wenn Sie ein Steuerelement deaktivieren, beendet Security Hub CSPM die Ausführung von Sicherheitsüberprüfungen und es werden keine Ergebnisse mehr generiert.

Sie können Kontrollen einzeln für ein einzelnes Konto aktivieren oder deaktivieren und. AWS-Region Um Zeit zu sparen und Konfigurationsabweichungen in Umgebungen mit mehreren Konten zu reduzieren, empfehlen wir, die Steuerung über eine [zentrale Konfiguration](#) zu aktivieren oder zu deaktivieren. Bei der zentralen Konfiguration kann der delegierte Security Hub CSPM-Administrator Richtlinien erstellen, die festlegen, wie eine Steuerung für mehrere Konten und Regionen konfiguriert werden soll. Weitere Informationen zum Aktivieren und Deaktivieren von Steuerungen finden Sie unter [Steuerelemente in Security Hub CSPM aktivieren](#)

Ansicht „Konsolidierte Kontrollen“

Auf der Seite „Steuerungen“ der Security Hub CSPM-Konsole werden alle derzeit verfügbaren Kontrollen angezeigt AWS-Region (Sie können Kontrollen im Kontext eines Standards anzeigen, indem Sie die Seite Sicherheitsstandards aufrufen und einen aktivierten Standard auswählen). Security Hub CSPM weist Kontrollen standardübergreifend eine einheitliche Sicherheitssteuerungs-ID, einen Titel und eine Beschreibung zu. Zu den Kontrollen IDs gehören die relevante AWS-Service und eine eindeutige Nummer (z. B. CodeBuild .3).

Die folgenden Informationen sind auf der Kontrollseite der [Security Hub CSPM-Konsole](#) verfügbar:

- Eine allgemeine Sicherheitsbewertung, die auf dem Anteil der bestandenen Kontrollen im Vergleich zur Gesamtzahl der aktivierten Kontrollen mit Daten basiert
- Aufschlüsselung der Kontrollstatus aller unterstützten Security Hub CSPM-Steuerungen

- Die Gesamtzahl der bestandenen und fehlgeschlagenen Sicherheitschecks.
- Die Anzahl der fehlgeschlagenen Sicherheitsüberprüfungen für Kontrollen mit unterschiedlichem Schweregrad sowie Links zu weiteren Informationen zu diesen fehlgeschlagenen Prüfungen.
- Eine Liste von Security Hub CSPM-Steuerelementen mit Filtern zur Anzeige bestimmter Untergruppen von Kontrollen.

Auf der Seite „Kontrollen“ können Sie ein Steuerelement auswählen, um dessen Details einzusehen und aufgrund der von der Kontrolle generierten Ergebnisse Maßnahmen zu ergreifen. Auf dieser Seite können Sie auch eine Sicherheitskontrolle in Ihrem aktuellen AWS-Konto und aktivieren oder deaktivieren AWS-Region. Die Aktivierungs- und Deaktivierungsaktionen auf der Seite „Kontrollen“ gelten für alle Standards. Weitere Informationen finden Sie unter [Steuerelemente in Security Hub CSPM aktivieren](#).

Bei Administratorkonten gibt die Seite „Kontrollen“ den Status der Kontrollen für alle Mitgliedskonten wieder. Wenn eine Kontrollüberprüfung in mindestens einem Mitgliedskonto fehlschlägt, lautet der Kontrollstatus Fehlgeschlagen. Wenn Sie eine [Aggregationsregion](#) festgelegt haben, zeigt die Seite „Steuerelemente“ den Status der Kontrollen in allen verknüpften Regionen an. Wenn eine Kontrollprüfung in mindestens einer verknüpften Region fehlschlägt, lautet der Kontrollstatus Fehlgeschlagen.

Die Ansicht „Konsolidierte Kontrollen“ führt zu Änderungen an den Kontrollsuchfeldern im AWS Security Finding Format (ASFF), die sich auf Workflows auswirken können. Weitere Informationen finden Sie unter [Ansicht konsolidierter Kontrollen — ASFF-Änderungen](#).

Zusammenfassung der Sicherheitsbewertung für Kontrollen

Auf der Seite „Kontrollen“ wird eine Zusammenfassung der Sicherheitsbewertung zwischen 0 und 100 Prozent angezeigt. Die zusammenfassende Sicherheitsbewertung wird auf der Grundlage des Anteils der bestandenen Kontrollen im Vergleich zur Gesamtzahl der aktivierten Kontrollen mit standardübergreifenden Daten berechnet.

Note

Um die Gesamtsicherheitsbewertung für Kontrollen anzuzeigen, müssen Sie der IAM-Rolle, die Sie für den **BatchGetControlEvaluations**-Zugriff auf Security Hub CSPM verwenden, die Berechtigung zum Aufrufen hinzufügen. Diese Berechtigung ist nicht erforderlich, um Sicherheitsbewertungen für bestimmte Standards einzusehen.

Wenn Sie Security Hub CSPM aktivieren, berechnet Security Hub CSPM die anfängliche Sicherheitsbewertung innerhalb von 30 Minuten nach Ihrem ersten Besuch der Übersichtsseite oder der Seite Sicherheitsstandards auf der Security Hub CSPM-Konsole. In den China Regionen und kann es bis zu 24 Stunden dauern, bis zum ersten Mal Sicherheitsbewertungen generiert werden. AWS GovCloud (US) Regions

Zusätzlich zur Gesamtsicherheitsbewertung berechnet Security Hub CSPM innerhalb von 30 Minuten nach Ihrem ersten Besuch der Übersichtsseite oder der Seite Sicherheitsstandards eine Standardsicherheitsbewertung für jeden aktivierten Standard. Verwenden Sie die API-Operation, um eine Liste der derzeit aktivierten Standards anzuzeigen. [GetEnabledStandards](#)

AWS Config Damit die Ergebnisse angezeigt werden, muss die Ressourcenaufzeichnung aktiviert sein. Informationen darüber, wie Security Hub CSPM Sicherheitsbewertungen berechnet, finden Sie unter. [Berechnung von Sicherheitswerten](#)

Nach der erstmaligen Score-Generierung aktualisiert Security Hub CSPM die Sicherheitswerte alle 24 Stunden. Security Hub CSPM zeigt einen Zeitstempel an, der angibt, wann eine Sicherheitsbewertung zuletzt aktualisiert wurde.

Wenn Sie eine Aggregationsregion festgelegt haben, spiegelt die Gesamtsicherheitsbewertung die Kontrollergebnisse der verknüpften Regionen wider.

Kontrollreferenz für Security Hub CSPM

Diese Kontrollreferenz enthält eine Tabelle der verfügbaren AWS Security Hub Cloud Security Posture Management (CSPM) -Steuerelemente mit Links zu weiteren Informationen zu den einzelnen Kontrollen. In der Tabelle sind die Kontrollen in alphabetischer Reihenfolge nach der Kontroll-ID aufgeführt. Nur Steuerelemente, die von Security Hub CSPM aktiv verwendet werden, sind hier enthalten. Steuerelemente, die nicht mehr verwendet wurden, sind in der Tabelle nicht enthalten.

Die Tabelle enthält die folgenden Informationen für jedes Steuerelement:

- ID der Sicherheitskontrolle — Diese ID gilt für alle Standards und gibt die AWS-Service Ressource an, auf die sich die Kontrolle bezieht. Die Security Hub CSPM-Konsole zeigt die Sicherheitskontrolle an IDs, unabhängig davon, ob die [konsolidierten Kontrollergebnisse](#) in Ihrem Konto aktiviert oder deaktiviert sind. Die CSPM-Ergebnisse von Security Hub beziehen sich jedoch IDs nur dann auf die Sicherheitskontrolle, wenn konsolidierte Kontrollergebnisse in Ihrem Konto aktiviert sind. Wenn die Option „Konsolidierte Kontrollfeststellungen“ in Ihrem Konto deaktiviert

ist, IDs variieren einige Kontrollen je nach Standard in Ihren Kontrollergebnissen. Eine Zuordnung zwischen standardspezifischer Kontrolle und Sicherheitskontrolle IDs finden Sie IDs unter. [Wie sich die Konsolidierung auf Kontrolle und Titel auswirkt IDs](#)

Wenn Sie [Automatisierungen](#) für Sicherheitskontrollen einrichten möchten, empfehlen wir, anhand der Kontroll-ID und nicht anhand des Titels oder der Beschreibung zu filtern. Security Hub CSPM kann zwar gelegentlich Titel oder Beschreibungen von Steuerelementen aktualisieren, die Steuerung IDs bleibt jedoch dieselbe.

Bei der Steuerung IDs können Zahlen übersprungen werden. Dies sind Platzhalter für future Kontrollen.

- Titel der Sicherheitskontrolle — Dieser Titel gilt für alle Standards. In der Security Hub CSPM-Konsole werden Titel der Sicherheitskontrollen angezeigt, unabhängig davon, ob konsolidierte Kontrollergebnisse in Ihrem Konto aktiviert oder deaktiviert sind. Die CSPM-Ergebnisse von Security Hub verweisen jedoch nur dann auf Titel der Sicherheitskontrolle, wenn konsolidierte Kontrollergebnisse in Ihrem Konto aktiviert sind. Wenn die Option „Konsolidierte Kontrollbefunde“ in Ihrem Konto deaktiviert ist, variieren einige Kontrolltitel je nach Standard in Ihren Kontrollergebnissen. Eine Zuordnung zwischen standardspezifischer Kontrolle und Sicherheitskontrolle IDs finden Sie IDs unter. [Wie sich die Konsolidierung auf Kontrolle und Titel auswirkt IDs](#)
- Anwendbare Standards — Gibt an, für welche Standards eine Kontrolle gilt. Wählen Sie eine Kontrolle aus, um bestimmte Anforderungen aus Compliance-Frameworks von Drittanbietern zu überprüfen.
- Schweregrad — Der Schweregrad einer Kontrolle gibt an, wie wichtig sie aus Sicherheitsgründen ist. Informationen darüber, wie Security Hub CSPM den Schweregrad der Kontrolle bestimmt, finden Sie unter. [Schweregrade der Kontrollbefunde](#)
- Unterstützt benutzerdefinierte Parameter — Gibt an, ob das Steuerelement benutzerdefinierte Werte für einen oder mehrere Parameter unterstützt. Wählen Sie ein Steuerelement aus, um die Parameterdetails zu überprüfen. Weitere Informationen finden Sie unter [Grundlegendes zu den Steuerparametern in Security Hub CSPM](#).
- Zeitplan — Gibt an, wann die Kontrolle ausgewertet wird. Weitere Informationen finden Sie unter [Zeitplan für die Ausführung von Sicherheitsprüfungen](#).

Wählen Sie ein Steuerelement aus, um weitere Details zu überprüfen. Die Kontrollen werden in alphabetischer Reihenfolge nach der Sicherheitskontroll-ID aufgelistet.

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Account.1	Sicherheitskontaktinformationen sollten für eine bereitgestellt werden AWS-Konto	CIS AWS Foundations Benchmark v3.0.0, Best Practices für AWS grundlegende Sicherheit v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
Konto.2	AWS-Konto sollte Teil einer Organisation sein AWS Organisations	NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Regelmäßig
ACM.1	Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MITTEL	 Ja	Änderung ausgelöst und periodisch
ACM.2	Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, PCI DSS v4.0.1	HIGH (HOCH)	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ACM.3	ACM-Zertifikate sollten gekennzeichnet sein	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
Verstärker.1	Amplify-Apps sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
Verstärker.2	Amplify-Zweige sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
APIGateway1.	API Gateway, REST und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
APIGateway2.2	API Gateway, REST-API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden.	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: NIST SP 800-53 AWS Control Tower Rev. 5, NIST SP 800-171 Rev. 2	MITTEL	 Nein	Änderung ausgelöst
APIGateway3.	Bei den REST-API-Stufen von API Gateway sollte die AWS X-Ray Ablaufverfolgung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
APIGateway4.	API Gateway sollte mit einer WAF-WebACL verknüpft sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
APIGateway5.	API-Gateway-REST-API-Cache-Daten sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
APIGateway8.	API-Gateway-Routen sollten einen Autorisierungstyp angeben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Regelmäßig
APIGateway9.	Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, NIST SP 800-53 AWS Control Tower Rev. 5, PCI DSS v4.0.1	MITTEL	 Nein	Änderung ausgelöst
AppConfig1.	AWS AppConfig Anwendungen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
AppConfig 2.2	AWS AppConfig Konfigurationsprofile sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
AppConfig 3.	AWS AppConfig Umgebungen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
AppConfig 4.	AWS AppConfig Erweiterungszuordnungen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
AppFlow1.	AppFlow Amazon-Datenflüsse sollten gekennzeichnet werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
AppRunner 1.	App Runner-Dienste sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
AppRunner 2.2	App Runner VPC-Konnektoren sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
AppSync1.	AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Änderung ausgelöst
AppSync2.2	AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, PCI DSS v4.0.1	MITTEL	 Ja	Änderung ausgelöst
AppSync4.	AWS AppSync GraphQL APIs sollte markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
AppSync5.	AWS AppSync GraphQL APIs sollte nicht mit API-Schlüsseln authentifiziert werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst
AppSync6.	AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Änderung ausgelöst
Athena.2	Athena-Datenkataloge sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Athena.3	Athena-Arbeitsgruppen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
Athena.4	Athena-Arbeitsgruppen sollte die Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Änderung ausgelöst
AutoScaling1.	Auto Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden	AWS Bewährte grundlegende Sicherheitsmethoden, Service-Managed-Standard, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
AutoScaling2.2	Die Amazon EC2 Auto Scaling-Gruppe sollte mehrere Availability Zones abdecken	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
AutoScaling3.	Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2 Instances so konfigurieren, dass sie Instance Metadata Service Version 2 (IMDSv2) benötigen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, NIST SP 800-53 AWS Control Tower Rev. 5, PCI DSS v4.0.1	HIGH (HOCH)	 Nein	Änderung ausgelöst
AutoScaling5.	EC2 Amazon-Instances, die mit Auto Scaling Scaling-Gruppenstartkonfigurationen gestartet wurden, sollten keine öffentlichen IP-Adressen haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, NIST SP 800-53 AWS Control Tower Rev. 5, PCI DSS v4.0.1	HIGH (HOCH)	 Nein	Änderung ausgelöst
AutoScaling6.	Auto Scaling Scaling-Gruppen sollten mehrere Instanztypen in mehreren Availability Zones verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
AutoScaling9.	EC2 Auto Scaling Scaling-Gruppen sollten EC2 Startvorlagen verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
AutoScaling1.0	EC2 Auto Scaling Scaling-Gruppen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
Sicherung.1	AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
Sicherung.2	AWS Backup Wiederherstellungspunkte sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
Sicherung.3	AWS Backup Tresore sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Sicherung.4	AWS Backup Berichtspläne sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
Sicherung.5	AWS Backup Backup-Pläne sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
Charge.1	Warteschlangen für Batch-Jobs sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
Charge.2	Richtlinien zur Batch-Planung sollten gekennzeichnet sein	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
Charge.3	Batch-Computing-Umgebungen sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Charge.4	Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
CloudFormation2.2	CloudFormation Stapel sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
CloudFront1.	CloudFront Bei Distributionen sollte ein Standard-Root-Objekt konfiguriert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	HIGH (HOCH)	 Nein	Änderung ausgelöst
CloudFront3.	CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudFront4.	CloudFront Bei Distributionen sollte Origin Failover konfiguriert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
CloudFront5.	CloudFront Bei Distributionen sollte die Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MITTEL	 Nein	Änderung ausgelöst
CloudFront6.	CloudFront Bei Distributionen sollte WAF aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MITTEL	 Nein	Änderung ausgelöst
CloudFront7.	CloudFront Distributionen sollten benutzerdefinierte Zertifikate verwenden SSL/TLS	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudFront t8.	CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
CloudFront t9.	CloudFront Distributionen sollten den Verkehr zu benutzerdefinierten Ursprüngen verschlüsseln	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MITTEL	 Nein	Änderung ausgelöst
CloudFront t1.0	CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MITTEL	 Nein	Änderung ausgelöst
CloudFront t1.2	CloudFront Verteilungen sollten nicht auf nicht existierende S3-Ursprünge verweisen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	HIGH (HOCH)	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudFront1.3	CloudFront Distributionen sollten Origin Access Control verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0	MITTEL	 Nein	Änderung ausgelöst
CloudFront1.4	CloudFront Distributionen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
CloudFront1.5	CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0	MITTEL	 Nein	Änderung ausgelöst
CloudTrail1.	CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungseignisse für Lese- und Schreibvorgänge umfasst	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit, Service-Managed Standard, NIST SP 800-53 Rev. 5 AWS Control Tower	HIGH (HOCH)	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudTrail I2.2	CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert sein	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0 Bewährte Methoden für grundlegende Sicherheit v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	MITTEL	 Nein	Regelmäßig
CloudTrail I3.	Mindestens ein CloudTrail Trail sollte aktiviert sein	NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, PCI DSS v3.2.1	HIGH (HOCH)	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudTrail I.4	CloudTrail Die Überprüfung der Protokolldatei sollte aktiviert sein	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, PCI DSS v3.2.1, Service-Managed Standard: AWS Control Tower	NIEDRIG	 Nein	Regelmäßig
CloudTrail I.5	CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden	CIS AWS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	NIEDRIG	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudTrail I6.	Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist	CIS AWS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0, PCI DSS v4.0.1	KRITISCH	 Nein	Änderung ausgelöst und periodisch
CloudTrail I7.	Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist	CIS AWS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v3.0.0, PCI DSS v4.0.1	NIEDRIG	 Nein	Regelmäßig
CloudTrail I9.	CloudTrail Wege sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
CloudTrail I1.0	CloudTrail Datenspeicher für Ereignisse in Lake sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys	NIST SP 800-53 Rev. 5	MITTEL	 Ja	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudWatch h1.	Für die Verwendung des Root-Benutzers sollten ein Log-Metrikfilter und ein Alarm vorhanden sein	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1	NIEDRIG	 Nein	Regelmäßig
CloudWatch h2.	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für nicht autorisierte API-Aufrufe vorhanden sind	Benchmark v1.2.0 für CIS AWS Foundations, NIST SP 800-171 Rev. 2	NIEDRIG	 Nein	Regelmäßig
CloudWatch h3.	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für die Anmeldung in der Managementkonsole ohne MFA vorhanden sind	Benchmark AWS v1.2.0 für CIS-Stiftungen	NIEDRIG	 Nein	Regelmäßig
CloudWatch h4.	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der IAM-Richtlinie vorhanden sind	Benchmark für AWS GIS-Stiftungen v1.4.0, Benchmark für AWS GIS-Stiftungen v1.2.0, NIST SP 800-171 Rev. 2	NIEDRIG	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudWatch h5.	Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für CloudTrail Konfigurationsänderungen vorhanden sind	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2	NIEDRIG	 Nein	Regelmäßig
CloudWatch h6.	Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Management Console Authentifizierungsfehler vorhanden sind	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2	NIEDRIG	 Nein	Regelmäßig
CloudWatch h7.	Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm vorhanden sind, um vom Kunden erstellte Dateien zu deaktivieren oder zu löschen CMKs	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2	NIEDRIG	 Nein	Regelmäßig
CloudWatch h8.	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der S3-Bucket-Richtlinie vorhanden sind	Benchmark für AWS GIS-Stiftungen v1.4.0, Benchmark für AWS GIS-Stiftungen v1.2.0, NIST SP 800-171 Rev. 2	NIEDRIG	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudWatch h9.	Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Config Konfigurationsänderungen vorhanden sind	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2	NIEDRIG	 Nein	Regelmäßig
CloudWatch h.10	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Sicherheitsgruppe vorhanden sind	Benchmark für AWS GUS-Stiftungen v1.4.0, Benchmark für AWS GUS-Stiftungen v1.2.0, NIST SP 800-171 Rev. 2	NIEDRIG	 Nein	Regelmäßig
CloudWatch h.11	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind	Benchmark für AWS GUS-Stiftungen v1.4.0, Benchmark für AWS GUS-Stiftungen v1.2.0, NIST SP 800-171 Rev. 2	NIEDRIG	 Nein	Regelmäßig
CloudWatch h1.2	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an Network-Gateways vorhanden sind	Benchmark für AWS GUS-Stiftungen v1.4.0, Benchmark für AWS GUS-Stiftungen v1.2.0, NIST SP 800-171 Rev. 2	NIEDRIG	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudWatch h1.3	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Routing-Tabelle vorhanden sind	Benchmark für AWS GUS-Stiftungen v1.4.0, Benchmark für AWS GUS-Stiftungen v1.2.0, NIST SP 800-171 Rev. 2	NIEDRIG	 Nein	Regelmäßig
CloudWatch h.14	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für VPC-Änderungen vorhanden sind	Benchmark für AWS GUS-Stiftungen v1.4.0, Benchmark für AWS GUS-Stiftungen v1.2.0, NIST SP 800-171 Rev. 2	NIEDRIG	 Nein	Regelmäßig
CloudWatch h.15	CloudWatch Für Alarme sollten bestimmte Aktionen konfiguriert sein	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	HIGH (HOCH)	 Ja	Änderung ausgelöst
CloudWatch h1.6	CloudWatch Protokollgruppen sollten für einen bestimmten Zeitraum aufbewahrt werden	NIST SP 800-53 Rev. 5	MITTEL	 Ja	Regelmäßig
CloudWatch h.17	CloudWatch Alarmaktionen sollten aktiviert sein	NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CodeArtifact1.	CodeArtifact Repositorien sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
CodeBuild1.	CodeBuild Das Bitbucket-Quell-Repository URLs sollte keine vertraulichen Anmeldeinformationen enthalten	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	KRITISCH	 Nein	Änderung ausgelöst
CodeBuild2.2	CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	KRITISCH	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CodeBuild 3.	CodeBuild S3-Protokolle sollten verschlüsselt sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed Standard:, AWS Control Tower	NIEDRIG	 Nein	Änderung ausgelöst
CodeBuild 4.	CodeBuild Projektumgebungen sollten über eine Protokollierungskonfiguration verfügen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
CodeBuild 7.	CodeBuild Exporte von Berichtsgruppen sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Änderung ausgelöst
CodeGuruProfiler 1.	CodeGuru Profiler-Profiling-Gruppen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CodeGuruReviewer1.	CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
Kognito.1	In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Ja	Änderung ausgelöst
Kognito.2	Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Änderung ausgelöst
Config.1	AWS Config sollte aktiviert sein und die serviceverknüpfte Rolle für die Ressourcenaufzeichnung verwenden	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1	KRITISCH	 Ja	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Verbinden.1	Die Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
Verbinden.2	Amazon Connect Connect-Instances sollte die CloudWatch Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Änderung ausgelöst
DataFirehose1.	Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
DataSync1.	DataSync Für Aufgaben sollte die Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Änderung ausgelöst
DataSync2.2	DataSync Aufgaben sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Detektiv.1	Verhaltensdiagramme von Detektiven sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
DMS.1	Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	KRITISCH	 Nein	Regelmäßig
DMS.2	DMS-Zertifikate sollten mit einem Tag versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
DMS.3	DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
DMS.4	DMS-Replikationsinstanzen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
DMS.5	Subnetzgruppen für die DMS-Replikation sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
DMS.6	Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MITTEL	 Nein	Änderung ausgelöst
DMS.7	Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MITTEL	 Nein	Änderung ausgelöst
DMS.8	Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MITTEL	 Nein	Änderung ausgelöst
DMS.9	DMS-Endpunkte sollten SSL verwenden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
DMS.10	Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MITTEL	 Nein	Änderung ausgelöst
DMS.11	Für DMS-Endpunkte für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MITTEL	 Nein	Änderung ausgelöst
DMS.12	Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MITTEL	 Nein	Änderung ausgelöst
DocumentDB DB.1	Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, Service-Managed Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
DocumentDB DB.2	Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	MITTEL	 Ja	Änderung ausgelöst
DocumentDB DB.3	Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	KRITISCH	 Nein	Änderung ausgelöst
DocumentDB DB.4	Amazon DocumentDB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MITTEL	 Nein	Änderung ausgelöst
DocumentDB DB.5	Für Amazon DocumentDB-Cluster sollte der Löschschutz aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
DocumentDB DB.6	Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
DynamoDB 1	DynamoDB-Tabellen sollten die Kapazität automatisch bei Bedarf skalieren	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Regelmäßig
DynamoDB 2	DynamoDB-Tabellen sollte die Wiederherstellung aktiviert point-in-time sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
DynamoDB 3	DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
DynamoDB.4	DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein	NIST SP 800-53 Rev. 5	MITTEL	 Ja	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
DynamoDB.5	DynamoDB-Tabellen sollten mit Tags versehen werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
DynamoDB.6	DynamoDB DynamoDB-Tabellen sollte der Löschschutz aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
DynamoDB.7	DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MITTEL	 Nein	Regelmäßig
EC2.1.	EBS-Snapshots sollten nicht öffentlich wiederherstellbar sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	KRITISCH	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC22.	VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, Service-Managed Standard, PCI DSS v3.2.1, CIS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5 AWS	HIGH (HOCH)	 Nein	Änderung ausgelöst
EC23.	Angehängte EBS-Volumes sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC24.	Gestoppte EC2 Instanzen sollten nach einem bestimmten Zeitraum entfernt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Regelmäßig
EC26.	Die VPC-Flow-Protokollierung sollte in allen aktiviert sein VPCs	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, Service-Managed Standard, PCI DSS v3.2.1 AWS Control Tower, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC27.	Die EBS-Standardverschlüsselung sollte aktiviert sein	CIS AWS Foundations Benchmark v3.0.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, Service-Managed Standard, CIS AWS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
EC28.	EC2 Instanzen sollten Instance Metadata Service Version 2 () IMDSv2 verwenden	CIS AWS Foundations Benchmark v3.0.0, Bewährte Methoden für AWS grundlegende Sicherheit, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	HIGH (HOCH)	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC29.	EC2 Instanzen sollten keine öffentliche IPv4 Adresse haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst
EC21.0	Amazon EC2 sollte für die Verwendung von VPC-Endpunkten konfiguriert sein, die für den Amazon-Service erstellt wurden EC2	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard:, NIST SP 800-53 Rev. 5, AWS Control Tower 5, NIST SP 800-171 Rev. 2	MITTEL	 Nein	Regelmäßig
EC21.2	Unbenutztes EC2 EIPs sollte entfernt werden	PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
EC21.3	Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen	CIS AWS Foundations Benchmark v1.2.0, PCI DSS v3.2.1, PCI DSS v4.0.1, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	HIGH (HOCH)	 Nein	Ausgelöst und periodische Änderung

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC21.4	Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 oder: :/0 auf Port 3389 zulassen	Benchmark für CIS Foundations v1.2.0 AWS , PCI DSS v4.0.1	HIGH (HOCH)	 Nein	Ausgelöst und periodische Änderung
EC21.5	EC2 Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed Standard:, AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
EC21.6	Unbenutzte Network Access Control Lists sollten entfernt werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, Service-Managed Standard:, AWS Control Tower	NIEDRIG	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC21.7	EC2 Instanzen sollten nicht mehrere verwenden ENIs	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
EC21.8	Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Verkehr für autorisierte Ports zulassen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard:, NIST SP 800-53 AWS Control Tower Rev. 5, NIST SP 800-171 Rev. 2	HIGH (HOCH)	 Ja	Änderung ausgelöst
EC21.9	Sicherheitsgruppen sollten keinen uneingeschränkten Zugriff auf Ports mit hohem Risiko zulassen	AWS Bewährte grundlegende Sicherheitsmethoden, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	KRITISCH	 Nein	Änderung ausgelöst und periodisch

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC22.0	Beide VPN-Tunnel für eine AWS Site-to-Site VPN-Verbindung sollten aktiv sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower, NIST SP 800-171 Rev. 2	MITTEL	 Nein	Änderung ausgelöst
EC22.1	ACLs Das Netzwerk sollte keinen Zugang von 0.0.0.0/0 zu Port 22 oder Port 3389 zulassen	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, Bewährte Methoden für AWS grundlegende Sicherheit, Service-Managed Standard:, NIST SP 800-53 Rev. 5, NIST SP 800-171 AWS Control Tower Rev. 2, PCI DSS v4.0.1	MITTEL	 Nein	Änderung ausgelöst
EC22.2	Unbenutzte EC2 Sicherheitsgruppen sollten entfernt werden	Vom Service verwalteter Standard: AWS Control Tower	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC22.3	EC2 Transit Gateways sollten VPC-Anhangsanfragen nicht automatisch akzeptieren	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst
EC22.4	EC2 Paravirtuelle Instanztypen sollten nicht verwendet werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
EC22.5	EC2 Startvorlagen sollten Netzwerkschnittstellen nicht öffentlich IPs zuweisen	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	HIGH (HOCH)	 Nein	Änderung ausgelöst
EC22.8	EBS-Volumes sollten in einem Backup-Plan enthalten sein	NIST SP 800-53 Rev. 5	NIEDRIG	 Ja	Regelmäßig
EC23.3	EC2 Transit-Gateway-Anhänge sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC23.4	EC2 Routentabellen für Transit-Gateways sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
EC23.5	EC2 Netzwerkschnittstellen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
EC23.6	EC2 Kunden-Gateways sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
EC23.7	EC2 Elastische IP-Adressen sollten mit Tags versehen werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
EC23.8	EC2 Instanzen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
EC23.9	EC2 Internet-Gateways sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC24.0	EC2 NAT-Gateways sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
EC24.1	EC2 Netzwerk ACLs sollte markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
EC24.2	EC2 Routentabellen sollten mit Tags versehen werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
EC24.3	EC2 Sicherheitsgruppen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
EC24.4	EC2 Subnetze sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
EC24.5	EC2 Bänder sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC24.6	Amazon VPCs sollte markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
EC24.7	Amazon VPC Endpoint Services sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
EC24.8	Amazon VPC-Flow-Logs sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
EC24.9	Amazon VPC-Peering-Verbindungen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
EC25.0	EC2 VPN-Gateways sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC25.1	EC2 Client-VPN-Endpunkte sollten die Client-Verbindungsprotokollierung aktiviert haben	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	NIEDRIG	 Nein	Änderung ausgelöst
EC25.2	EC2 Transit-Gateways sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
EC25.3	EC2 Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 auf die Verwaltungsports des Remoteservers zulassen	Benchmark für CIS AWS Foundations v3.0.0, PCI DSS v4.0.1	HIGH (HOCH)	 Nein	Regelmäßig
EC25.4	EC2 Sicherheitsgruppen sollten keinen Zugriff von: :/0 zu Remoteserver-Verwaltungsports zulassen	Benchmark für CIS AWS Foundations v3.0.0, PCI DSS v4.0.1	HIGH (HOCH)	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC25.5	VPCs sollte mit einem Schnittstellenendpunkt für die ECR-API konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Regelmäßig
EC25.6	VPCs sollte mit einem Schnittstellenendpunkt für Docker Registry konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Regelmäßig
EC25.7	VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Regelmäßig
EC25.8	VPCs sollte mit einem Schnittstellen-Endpunkt für Systems Manager Incident Manager Kontakte konfiguriert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Regelmäßig
EC26.0	VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC2.170	EC2 Startvorlagen sollten Instance Metadata Service Version 2 () IMDSv2 verwenden	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1	NIEDRIG	 Nein	Änderung ausgelöst
EC2.171	EC2 Bei VPN-Verbindungen sollte die Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1	MITTEL	 Nein	Änderung ausgelöst
EC2.172	EC2 Die Einstellungen für VPC Block Public Access sollten den Internet-Gateway-Verkehr blockieren	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Ja	Änderung ausgelöst
EC2.173	EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Änderung ausgelöst
EC2.174	EC2 DHCP-Optionssätze sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC2.175	EC2 Startvorlagen sollten markiert sein	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
EC2.176	EC2 Präfixlisten sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
EC2.177	EC2 Traffic Mirror-Sitzungen sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
EC2.178	EC2 Filter für Verkehrsspiegel sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
EC2.179	EC2 Verkehrsspiegelziele sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
EC2.180	EC2 Bei Netzwerkschnittstellen sollte die source/destination Überprüfung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ECR.1	Für private ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed-Standard: AWS Control Tower	HIGH (HOCH)	 Nein	Regelmäßig
ECR.2	Für private ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
ECR.3	Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
ECR.4	Öffentliche ECR-Repositoryn sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ECR.5	ECR-Repositorys sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys	NIST SP 800-53 Rev. 5	MITTEL	 Ja	Änderung ausgelöst
ECS.1	Amazon ECS-Aufgabendefinitionen sollten sichere Netzwerkmodi und Benutzerdefinitionen enthalten.	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst
ECS.2	ECS-Diensten sollten nicht automatisch öffentliche IP-Adressen zugewiesen werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	HIGH (HOCH)	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ECS.3	ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst
ECS.4	ECS-Container sollten ohne Zugriffsrechte ausgeführt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst
ECS.5	ECS-Container sollten auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	HIGH (HOCH)	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ECS.8	Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed-Standard: AWS Control Tower	HIGH (HOCH)	 Nein	Änderung ausgelöst
ECS.9	ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst
ECS.10	Die ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion ausgeführt werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ECS.12	ECS-Cluster sollten Container Insights verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
ECS.13	ECS-Dienste sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
ECS.14	ECS-Cluster sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
ECS.15	ECS-Aufgabendefinitionen sollten mit einem Tag versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
ECS.16	ECS-Aufgabensätze sollten öffentliche IP-Adressen nicht automatisch zuweisen	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1	HIGH (HOCH)	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ECS.17	ECS-Aufgabendefinitionen sollten nicht den Host-Netzwerkmodus verwenden	NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
EFS.1	Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS	CIS AWS Foundations Benchmark v3.0.0, Best Practices für AWS grundlegende Sicherheit v1.0.0, Service-Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MITTEL	 Nein	Regelmäßig
EFS.2	Amazon EFS-Volumen sollten in Backup-Plänen enthalten sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EFS.3	EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
EFS.4	EFS-Zugriffspunkte sollten eine Benutzeridentität erzwingen	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
EFS.5	EFS-Zugangspunkte sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
EFS.6	EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EFS.7	EFS-EFS-Dateisystemen sollten automatische Backups aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Änderung ausgelöst
EFS.8	EFS-Dateisysteme sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Ja	Änderung ausgelöst
EKS.1	EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	HIGH (HOCH)	 Nein	Regelmäßig
EKS.2	EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed-Standard: AWS Control Tower	HIGH (HOCH)	 Nein	Änderung ausgelöst
EKS.3	EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EKS. 6	EKS-Cluster sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
EKS.7	Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
EKS.8	Bei EKS-Clustern sollte die Auditprotokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MITTEL	 Nein	Änderung ausgelöst
ElastiCache1.	ElastiCache Bei Clustern (Redis OSS) sollten automatische Backups aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Ja	Regelmäßig
ElastiCache2.2	ElastiCache Bei Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	HIGH (HOCH)	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ElastiCache3.	ElastiCache Für Replikationsgruppen sollte automatisches Failover aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
ElastiCache4.	ElastiCache Replikationsgruppen sollten encrypted-at-rest	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
ElastiCache5.	ElastiCache Replikationsgruppen sollten encrypted-in-transit	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MITTEL	 Nein	Regelmäßig
ElastiCache6.	ElastiCache (Redis OSS) -Replikationsgruppen früherer Versionen sollten Redis OSS AUTH aktiviert haben	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MITTEL	 Nein	Regelmäßig
ElastiCache7.	ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ElasticBeanstalk1.	In Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
ElasticBeanstalk2.2	Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed-Standard: AWS Control Tower	HIGH (HOCH)	 Ja	Änderung ausgelöst
ElasticBeanstalk3.	Elastic Beanstalk sollte Logs streamen nach CloudWatch	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1	HIGH (HOCH)	 Ja	Änderung ausgelöst
ELB.1	Der Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ELB.2	Classic Load Balancer mit SSL/HTTPS Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, NIST SP 800-53 Rev. AWS Control Tower 5, NIST SP 800-171 Rev. 2	MITTEL	 Nein	Änderung ausgelöst
ELB.3	Classic Load Balancer Balancer-Listener sollten mit HTTPS- oder TLS-Terminierung konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
ELB.4	Der Application Load Balancer sollte so konfiguriert sein, dass er HTTP-Header löscht	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed-Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ELB.5	Die Protokollierung von Anwendungen und Classic Load Balancers sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
ELB.6	Für Anwendung, Gateway und Network Load Balancer sollte der Löschschutz aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
ELB.7	Bei Classic Load Balancers sollte der Verbindungsabbau aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ELB.8	Classic Load Balancer mit SSL-Listnern sollten eine vordefinierte Sicherheitsrichtlinie mit starker Konfiguration verwenden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
ELB.9	Bei Classic Load Balancern sollte der zonenübergreifende Load Balancing aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
ELB.10	Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ELB.12	Der Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden.	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed-Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
ELB.13	Load Balancer für Anwendungen, Netzwerke und Gateways sollten sich über mehrere Availability Zones erstrecken	AWS Bewährte grundlegende Sicherheitsmethode n v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Änderung ausgelöst
ELB.14	Der Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethode n, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ELB.16	Application Load Balancer sollten mit einer AWS WAF-Web-ACL verknüpft sein	NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
ELB.17	Anwendungs- und Netzwerk-Load-Balancer mit Listnern sollten die empfohlenen Sicherheitsrichtlinien verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
ELB.18	Applications- und Network Load Balancer Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln.	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0	MITTEL	 Nein	Änderung ausgelöst
EMR.1	Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	HIGH (HOCH)	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EMR. 2	Die Einstellung „Öffentlichen Zugriff blockieren“ in Amazon EMR sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	KRITISCH	 Nein	Regelmäßig
EMR. 3	Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
EMR. 4	Amazon EMR-Sicherheitskonfigurationen sollten bei der Übertragung verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
ES.1	Für Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ES.2	Elasticsearch-Domänen sollten nicht öffentlich zugänglich sein	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v3.2.1, PCI DSS v4.0.1, NIST SP 800-53 Rev. 5, Service-Managed Standard: AWS Control Tower	KRITISCH	 Nein	Regelmäßig
ES.3	Elasticsearch-Domänen sollten Daten verschlüsseln, die zwischen Knoten gesendet werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed Standard:, AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
ES.4	Die Protokollierung von Elasticsearch-Domänenfehlern in CloudWatch Logs sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ES.5	Für Elasticsearch-Domains sollte die Audit-Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, Service-Managed-Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
ES.6	Elasticsearch-Domains sollten mindestens drei Datenknoten haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
ES.7	Elasticsearch-Domains sollten mit mindestens drei dedizierten Master-Knoten konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ES.8	Verbindungen zu Elasticsearch-Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
ES.9	Elasticsearch-Domains sollten mit Tags versehen werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
EventBridge2.2	EventBridge Eventbusse sollten gekennzeichnet sein	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
EventBridge3.	EventBridge maßgeschneiderte Eventbusse sollten mit einer ressourcenbasierten Richtlinie versehen sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	NIEDRIG	 Nein	Änderung ausgelöst
EventBridge4.	EventBridge Auf globalen Endpunkten sollte die Ereignisreplikation aktiviert sein	NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
FraudDetector1.	Die Entitätstypen von Amazon Fraud Detector sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
FraudDetector2.2	Die Labels von Amazon Fraud Detector sollten gekennzeichnet sein	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
FraudDetector3.	Die Ergebnisse von Amazon Fraud Detector sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
FraudDetector4.	Die Variablen von Amazon Fraud Detector sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
FSx1.	FSx für OpenZFS sollten Dateisysteme so konfiguriert sein, dass sie Tags auf Backups und Volumes kopieren	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
FSx2.	FSx für Lustre-Datensysteme sollten so konfiguriert sein, dass sie Tags in Backups kopieren	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Regelmäßig
FSx3.	FSx für OpenZFS sollten Dateisysteme für den Multi-AZ-Einsatz konfiguriert sein	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Regelmäßig
FSx4.	FSx für NetApp ONTAP sollten Dateisysteme für den Multi-AZ-Einsatz konfiguriert sein	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Ja	Regelmäßig
FSx5.	FSx für Windows-Dateiserver sollten Dateisysteme für die Multi-AZ-Bereitstellung konfiguriert sein	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Regelmäßig
Kleber.1	AWS Glue Jobs sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Kleber.3	AWS Glue Transformationen für maschinelles Lernen sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Änderung ausgelöst
Kleber.4	AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
GlobalAccelerator1.	Global Accelerator-Beschleuniger sollten markiert sein	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
GuardDuty1.	GuardDuty sollte aktiviert sein	AWS Bewährte Methoden für grundlegende Sicherheit, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	HIGH (HOCH)	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
GuardDuty 2.2	GuardDuty Filter sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
GuardDuty 3.	GuardDuty IPSets sollte markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
GuardDuty 4.	GuardDuty Detektoren sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
GuardDuty 5.	GuardDuty EKS Audit Log Monitoring sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden	HIGH (HOCH)	 Nein	Regelmäßig
GuardDuty 6.	GuardDuty Lambda-Schutz sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1	HIGH (HOCH)	 Nein	Regelmäßig
GuardDuty 7.	GuardDuty EKS Runtime Monitoring sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
GuardDuty 8.	GuardDuty Der Malware-Schutz für EC2 sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden	HIGH (HOCH)	 Nein	Regelmäßig
GuardDuty 9.	GuardDuty Der RDS-Schutz sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1	HIGH (HOCH)	 Nein	Regelmäßig
GuardDuty 1.0	GuardDuty S3-Schutz sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1	HIGH (HOCH)	 Nein	Regelmäßig
GuardDuty 1.1	GuardDuty Runtime Monitoring sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden	HIGH (HOCH)	 Nein	Regelmäßig
GuardDuty 1.2	GuardDuty ECS Runtime Monitoring sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Regelmäßig
GuardDuty 1.3	GuardDuty EC2 Runtime Monitoring sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IAM.1	IAM-Richtlinien sollten keine vollen „*“ - Administratorrechte zulassen	CIS AWS Foundations Benchmark v1.2.0, Best Practices für AWS grundlegende Sicherheit v1.0.0, Service-Managed Standard, PCI DSS v3.2.1 AWS Control Tower, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	HIGH (HOCH)	 Nein	Änderung ausgelöst
IAM.2	IAM-Benutzern sollten keine IAM-Richtlinien zugewiesen sein	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, Service-Managed Standard, PCI DSS v3.2.1, NIST SP AWS Control Tower 800-53 Rev. 5, NIST SP 800-171 Rev. 2	NIEDRIG	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IAM.3	Die Zugangsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	MITTEL	 Nein	Regelmäßig
IAM.4	Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, Service-Managed Standard:, PCI DSS v3.2.1, NIST SP 800-53 Rev. AWS Control Tower 5	KRITISCH	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IAM.5	MFA sollte für alle IAM-Benutzer aktiviert sein, die ein Konsolenpasswort haben	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	MITTEL	 Nein	Regelmäßig
IAM.6	Hardware-MFA sollte für den Root-Benutzer aktiviert sein	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	KRITISCH	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IAM.7	Passwortrichtlinien für IAM-Benutzer sollten starke Konfigurationen haben	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	MITTEL	 Ja	Regelmäßig
IAM.8	Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden	CIS AWS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IAM.9	MFA sollte für den Root-Benutzer aktiviert sein	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	KRITISCH	 Nein	Regelmäßig
ICH.BIN.10	Passwortrichtlinien für IAM-Benutzer sollten solide Konfigurationen haben	NIST SP 800-171 Rev. 2, PCI DSS v3.2.1	MITTEL	 Nein	Regelmäßig
IAM.11	Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert	Benchmark der CIS AWS Foundations v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MITTEL	 Nein	Regelmäßig
IAM.12	Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert	Benchmark der CIS AWS Foundations v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IAM.13	Stellen Sie sicher, dass für die IAM-Passwortrichtlinie mindestens ein Symbol erforderlich ist	Benchmark v1.2.0 der CIS AWS Foundations, NIST SP 800-171 Rev. 2	MITTEL	 Nein	Regelmäßig
IAM.14	Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert	CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MITTEL	 Nein	Regelmäßig
IAM.15	Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2	MITTEL	 Nein	Regelmäßig
IAM.16	Sicherstellen, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert	Benchmark für AWS GUS-Stiftungen v3.0.0, Benchmark für AWS GUS-Stiftungen v1.4.0, Benchmark für AWS GIS-Stiftungen v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	NIEDRIG	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IAM.17	Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft	Benchmark v1.2.0 der CIS AWS Foundations, PCI DSS v4.0.1	NIEDRIG	 Nein	Regelmäßig
IAM.18	Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	NIEDRIG	 Nein	Regelmäßig
ICH BIN.19	MFA sollte für alle IAM-Benutzer aktiviert sein	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IAM.21	Von Ihnen erstellte, vom Kunden verwaltete IAM-Richtlinien sollten keine Platzhalteraktionen für Dienste zulassen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, NIST SP 800-53 Rev. AWS Control Tower 5, NIST SP 800-171 Rev. 2	NIEDRIG	 Nein	Änderung ausgelöst
IAM.22	IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-171 Rev. 2	MITTEL	 Nein	Regelmäßig
ICH BIN. 23	IAM Access Analyzer-Analyser sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
ICH BIN. 24	IAM-Rollen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
ICH BIN. 25	IAM-Benutzer sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ICH BIN .26	Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden	Benchmark v3.0.0 der CIS AWS Foundations	MITTEL	 Nein	Regelmäßig
ICH BIN. 27	IAM-Identitäten sollte die Richtlinie nicht beigefügt sein AWS Cloud Shell Full Access	Benchmark v3.0.0 für CIS AWS Foundations	MITTEL	 Nein	Änderung ausgelöst
ICH BIN .28	Der externe Zugriffsanalysator von IAM Access Analyzer sollte aktiviert sein	Benchmark AWS v3.0.0 für CIS Foundations	HIGH (HOCH)	 Nein	Regelmäßig
Inspektor .1	Das EC2 Scannen mit Amazon Inspector sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1	HIGH (HOCH)	 Nein	Regelmäßig
Inspektor .2	Das Amazon Inspector ECR-Scannen sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1	HIGH (HOCH)	 Nein	Regelmäßig
Inspektor .3	Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1	HIGH (HOCH)	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Inspector.4	Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1	HIGH (HOCH)	 Nein	Regelmäßig
IoT.1	AWS IoT Device Defender Sicherheitsprofile sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
IoT.2	AWS IoT Core Maßnahmen zur Schadensbegrenzung sollten gekennzeichnet werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
IoT.3	AWS IoT Core Abmessungen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
IoT.4	AWS IoT Core Autorisierer sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
IoT.5	AWS IoT Core Rollenalias sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IoT. 6	AWS IoT Core Richtlinien sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
iOS TEvents 1.	AWS IoT Events Eingaben sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
iOS TEvents 1.2	AWS IoT Events Detektormodelle sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
iOS TEvents 3.	AWS IoT Events Alarmmodelle sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
Ich TSite weise.1	AWS IoT SiteWise Asset-Modelle sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
Ich TSite weise.2	AWS IoT SiteWise Dashboards sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Ich TSiteweise.3	AWS IoT SiteWise Gateways sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
Ich TSiteweise.4	AWS IoT SiteWise Portale sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
Ich TSiteweise.5	AWS IoT SiteWise Projekte sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
Io TTwinMaker.1	AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
Io TTwinMaker.2	AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
Io TTwinMaker.3	AWS TwinMaker IoT-Szenen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IoT TwinMaker.4	AWS TwinMaker IoT-Entitäten sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
IoT Wireless 1.	AWS IoT-Wireless-Multicast-Gruppen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
IoT Wireless 1.2	AWS IoT-Wireless-Dienstprofile sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
IoT Wireless 3.	AWS IoT Wireless FUOTA-Aufgaben sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
IVS.1	Schlüsselpaare für die IVS-Wiedergabe sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
IVS.2	IVS-Aufnahmekonfigurationen sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IVS.3	IVS-Kanäle sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
Tastenfelder.1	Amazon Keyspaces-Keyspaces sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
Kinesis.1	Kinesis-Streams sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
Kinesis.2	Kinesis-Streams sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
Kinesis.3	Kinesis-Streams sollten über eine angemessene Datenaufbewahrungsfrist verfügen	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
KMS.1	Vom Kunden verwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
KMS.2	IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
KMS.3	AWS KMS keys sollte nicht ungewollt gelöscht werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	KRITISCH	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
KMS.4	AWS KMS key Die Rotation sollte aktiviert sein	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	MITTEL	 Nein	Regelmäßig
KMS.5	KMS-Schlüssel sollten nicht öffentlich zugänglich sein	AWS Bewährte grundlegende Sicherheitsmethoden	KRITISCH	 Nein	Änderung ausgelöst
Lambda.1	Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	KRITISCH	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Lambda.2	Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed-Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
Lambda.3	Lambda-Funktionen sollten sich in einer VPC befinden	PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
Lambda.5	VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Änderung ausgelöst
Lambda.6	Lambda-Funktionen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Lambda.7	Lambda Lambda-Funktionen sollte die AWS X-Ray aktive Ablaufverfolgung aktiviert sein	NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
Macie.1	Amazon Macie sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
Macie.2	Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Regelmäßig
MSK.1	MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MITTEL	 Nein	Änderung ausgelöst
MSK.2	Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein	NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
MSK.3	MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1	MITTEL	 Nein	Änderung ausgelöst
MSK.4	Bei MSK-Clustern sollte der öffentliche Zugriff deaktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden	KRITISCH	 Nein	Änderung ausgelöst
MSK.5	Bei MSK-Anschlüssen sollte die Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Änderung ausgelöst
MSK.6	MSK-Cluster sollten den nicht authentifizierten Zugriff deaktivieren	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Änderung ausgelöst
MQ. 2	ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MITTEL	 Nein	Änderung ausgelöst
MQ. 3	Amazon MQ-Broker sollten das automatische Upgrade der Nebenversion aktiviert haben	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	NIEDRIG	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
MQ.4	Amazon MQ-Broker sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
MQ.5	ActiveMQ-Broker sollten den Bereitstellungsmodus verwenden active/standby	NIST SP 800-53 Rev. 5, vom Service verwalteter Standard: AWS Control Tower	NIEDRIG	 Nein	Änderung ausgelöst
MQ.6	RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden	NIST SP 800-53 Rev. 5, vom Service verwalteter Standard: AWS Control Tower	NIEDRIG	 Nein	Änderung ausgelöst
Neptun.1	Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, Service-Managed Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Neptun.2	Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
Neptun.3	Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	KRITISCH	 Nein	Änderung ausgelöst
Neptun.4	Neptune Neptune-DB-Clustern sollte der Löschschutz aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, Service-Managed Standard: AWS Control Tower	NIEDRIG	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Neptun.5	Neptune Neptune-DB-Clustern sollten automatische Backups aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, Service-Managed Standard: AWS Control Tower	MITTEL	 Ja	Änderung ausgelöst
Neptun.6	Neptune DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, Service-Managed Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
Neptun.7	Neptune Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, Service-Managed-Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Neptun.8	Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, Service-Managed Standard: AWS Control Tower	NIEDRIG	 Nein	Änderung ausgelöst
Neptun.9	Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden	NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
NetworkFirewall1.	Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden	NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
NetworkFirewall2.2	Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
NetworkFirewall3.	Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower, NIST SP 800-171 Rev. 2	MITTEL	 Nein	Änderung ausgelöst
NetworkFirewall4.	Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ lauten.	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
NetworkFirewall5.	Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ lauten.	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, NIST SP 800-53 Rev. 5, AWS Control Tower 5, NIST SP 800-171 Rev. 2	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
NetworkFirewall6.	Die Regelgruppe der Stateless Network Firewall sollte nicht leer sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard:, NIST SP 800-53 AWS Control Tower Rev. 5, NIST SP 800-171 Rev. 2	MITTEL	 Nein	Änderung ausgelöst
NetworkFirewall7.	Netzwerk-Firewall-Firewalls sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
NetworkFirewall8.	Netzwerk-Firewall-Firewall-Richtlinien sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
NetworkFirewall9.	Network Firewall Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
NetworkFirewall1.0	Network Firewall Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
OpenSearch h.1	OpenSearch Bei Domänen sollte die Verschlüsselung im Ruhezustand aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, PCI DSS AWS Control Tower v3.2.1, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
OpenSearch h.2	OpenSearch Domains sollten nicht öffentlich zugänglich sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, PCI DSS AWS Control Tower v3.2.1, NIST SP 800-53 Rev. 5	KRITISCH	 Nein	Änderung ausgelöst
OpenSearch h.3	OpenSearch Domänen sollten Daten verschlüsseln, die zwischen Knoten gesendet werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
OpenSearch h.4	OpenSearch Die Protokollierung von Domänenfehlern in CloudWatch Logs sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
OpenSearch h.5	OpenSearch Für Domänen sollte die Auditprotokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed-Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
OpenSearch h.6	OpenSearch Domänen sollten mindestens drei Datenknoten haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
OpenSearch h.7	OpenSearch Für Domänen sollte eine fein abgestufte Zugriffskontrolle aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst
OpenSearch h.8	Verbindungen zu OpenSearch Domänen sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
Suche öffnen.9	OpenSearch Domains sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
Suche öffnen.10	OpenSearch Auf den Domains sollte das neueste Softwareupdate installiert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	NIEDRIG	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Opensearch.h.11	OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben	NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Regelmäßig
PCA.1	AWS Private CA Die Stammzertifizierungsstelle sollte deaktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Regelmäßig
PCA.2	AWS Private Zertifizierungsstellen sollten gekennzeichnet werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
RDS.1	Der RDS-Snapshot sollte privat sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, PCI DSS AWS Control Tower v3.2.1, NIST SP 800-53 Rev. 5	KRITISCH	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.2	RDS-DB-Instances sollten, wie in der Konfiguration festgelegt, den PubliclyAccessible öffentlichen Zugriff verbieten	CIS AWS Foundations Benchmark v3.0.0, Bewährte Methoden für AWS grundlegende Sicherheit, Service-Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower, PCI DSS v3.2.1, PCI DSS v4.0.1	KRITISCH	 Nein	Änderung ausgelöst
RDS.3	Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, Service-Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.4	RDS-Cluster-Snapshots und Datenbank-Snapshots sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
RDS.5	RDS-DB-Instances sollten mit mehreren Availability Zones konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
RDS.6	Die erweiterte Überwachung sollte für RDS-DB-Instances konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.7	Bei RDS-Clustern sollte der Löschschutz aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
RDS.8	Für RDS-DB-Instances sollte der Löschschutz aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
RDS.9	RDS-DB-Instances sollten CloudWatch Protokolle in Logs veröffentlichen	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed-Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.10	Die IAM-Authentifizierung sollte für RDS-Instances konfiguriert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
RDS.11	Für RDS-Instances sollten automatische Backups aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Änderung ausgelöst
RDS.12	Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.13	Automatische RDS-Upgrades für kleinere Versionen sollten aktiviert sein	CIS AWS Foundations Benchmark v3.0.0, Bewährte Methoden für AWS grundlegende Sicherheit, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	HIGH (HOCH)	 Nein	Änderung ausgelöst
RDS.14	Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Änderung ausgelöst
RDS.15	RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
RDS.16	Aurora-DB-Cluster sollten so konfiguriert sein, dass sie Tags in DB-Snapshots kopieren	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.17	RDS-DB-Instances sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
RDS.18	RDS-Instances sollten in einer VPC bereitgestellt werden	Vom Service verwalteter Standard: AWS Control Tower	HIGH (HOCH)	 Nein	Änderung ausgelöst
RDS.19	Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Clusterereignisse konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
RDS.20	Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Ereignisse der Datenbankinstanz konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	NIEDRIG	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.21	Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbankparametergruppeneignisse konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	NIEDRIG	 Nein	Änderung ausgelöst
RDS.22	Für kritische Ereignisse in Datenbanksicherheitsgruppen sollte ein Abonnement für RDS-Ereignisbenachrichtigungen konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	NIEDRIG	 Nein	Änderung ausgelöst
RDS.23	RDS-Instances sollten keinen Standard-Port für die Datenbank-Engine verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.24	RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MITTEL	 Nein	Änderung ausgelöst
RDS.25	RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
RDS.26	RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden	NIST SP 800-53 Rev. 5	MITTEL	 Ja	Regelmäßig
RDS.27	RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, Service-Managed Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.28	RDS-DB-Cluster sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
RDS.29	Snapshots des RDS-DB-Clusters sollten mit Tags versehen werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
RDS.30	RDS-DB-Instances sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
RDS.31	RDS-DB-Sicherheitsgruppen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
RDS.32	RDS-DB-Snapshots sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
RDS.33	RDS-DB-Subnetzgruppen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.34	Aurora MySQL-DB-Cluster sollten Audit-Logs in CloudWatch Logs veröffentlichen	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MITTEL	 Nein	Änderung ausgelöst
RDS.35	Für RDS-DB-Cluster sollte das automatische Upgrade der Nebenversionen aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MITTEL	 Nein	Änderung ausgelöst
RDS.36	RDS für PostgreSQL-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1	MITTEL	 Ja	Änderung ausgelöst
RDS.37	Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1	MITTEL	 Nein	Änderung ausgelöst
RDS.38	RDS für PostgreSQL-DB-Instances sollten bei der Übertragung verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.39	RDS für MySQL-DB-Instances sollte bei der Übertragung verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Regelmäßig
RDS.40	RDS für SQL Server-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Änderung ausgelöst
RDS.41	RDS für SQL Server-DB-Instances sollten bei der Übertragung verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Regelmäßig
RDS.42	RDS für MariaDB-DB-Instances sollte Protokolle in Logs veröffentlichen CloudWatch	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Regelmäßig
RDS.44	RDS für MariaDB-DB-Instances sollte bei der Übertragung verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.45	Bei Aurora MySQL-DB-Clustern sollte die Audit-Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
Redshift.1	Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	KRITISCH	 Nein	Änderung ausgelöst
Redshift.2	Verbindungen zu Amazon Redshift Redshift-Clustern sollten während der Übertragung verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
Redshift.3	Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Redshift. 4	Amazon Redshift Redshift-Cluster sollte die Audit-Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
Redshift. 6	Bei Amazon Redshift sollten automatische Upgrades auf Hauptversionen aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
Redshift. 7	Redshift-Cluster sollten erweitertes VPC-Routing verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Redshift.8	Amazon Redshift Redshift-Cluster sollten nicht den standardmäßigen Admin-Benutzernamen verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
Redshift.9	Redshift-Cluster sollten nicht den Standarddatenbanknamen verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
Redshift.10	Redshift-Cluster sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
Rotverschlebung.11	Redshift-Cluster sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Rotverschlebung.12	Abonnementbenachrichtigungen für Redshift-Ereignisse sollten mit Tags versehen werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
Rotverschlebung.13	Redshift-Cluster-Snapshots sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
Rotverschlebung.14	Redshift-Cluster-Subnetzgruppen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
Rotverschlebung.15	Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Ursprüngen zulassen	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1	HIGH (HOCH)	 Nein	Regelmäßig
Rotverschlebung.16	Redshift-Cluster-Subnetzgruppen sollten Subnetze aus mehreren Availability Zones haben	NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Rotverschlebung.17	Redshift-Cluster-Parametergruppen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
Rotverschlebung.18	Redshift Redshift-Cluster sollten Multi-AZ-Bereitstellungen aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Änderung ausgelöst
RedshiftServerless 1.	Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden	AWS Bewährte grundlegende Sicherheitsmethoden	HIGH (HOCH)	 Nein	Regelmäßig
RedshiftServerless 2.2	Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Regelmäßig
RedshiftServerless 3.	Redshift Serverlose Arbeitsgruppen sollten den öffentlichen Zugriff verbieten	AWS Bewährte grundlegende Sicherheitsmethoden	HIGH (HOCH)	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RedshiftServerless 4.	Serverlose Redshift-Namespace sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys	NIST SP 800-53 Rev. 5	MITTEL	 Ja	Regelmäßig
RedshiftServerless 5.	Redshift Serverless-Namespace sollten nicht den Standard-Admin-Benutzernamen verwenden	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Ja	Regelmäßig
RedshiftServerless 6.	Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Regelmäßig
RedshiftServerless 7.	Redshift Serverless-Namespace sollten nicht den Standard-Datenbanknamen verwenden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
Route 53.1	Route 53-Gesundheitschecks sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Route 53.2	In öffentlich gehosteten Zonen von Route 53 sollten DNS-Abfragen protokolliert werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MITTEL	 Nein	Änderung ausgelöst
S3.1	Für S3-Allzweck-Buckets sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, Bewährte Methoden für AWS grundlegende Sicherheit, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	MITTEL	 Nein	Regelmäßig
S3.2	S3-Buckets für allgemeine Zwecke sollten den öffentlichen Lesezugriff blockieren	AWS Bewährte grundlegende Sicherheitsmethoden, Service-Managed Standard, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	KRITISCH	 Nein	Änderung ausgelöst und periodisch

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
S3.3	S3-Buckets für allgemeine Zwecke sollten den öffentlichen Schreibzugriff blockieren	AWS Bewährte grundlegende Sicherheitsmethoden, Service-Managed-Standard, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	KRITISCH	 Nein	Änderung ausgelöst und periodisch
S3.5	Für S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erforderlich sein	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, Bewährte Methoden für AWS grundlegende Sicherheit, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
S3.6	Allgemeine S3-Bucket-Richtlinien sollten den Zugriff auf andere einschränken AWS-Konten	AWS Bewährte grundlegende Sicherheitsmethoden, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	HIGH (HOCH)	 Nein	Änderung ausgelöst
S3.7	S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden	PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
S3.8	S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, Bewährte Methoden für AWS grundlegende Sicherheit, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	HIGH (HOCH)	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
S3.9	Für S3-Allzweck-Buckets sollte die Serverzugriffsprotokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
S3.10	S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben	NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
S3.11	Für S3-Buckets für allgemeine Zwecke sollten Ereignisbenachrichtigungen aktiviert sein	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MITTEL	 Ja	Änderung ausgelöst
S3.12	ACLs sollte nicht zur Verwaltung des Benutzerzugriffs auf S3-Allzweck-Buckets verwendet werden	AWS Bewährte grundlegende Sicherheitsmethoden, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
S3.13	S3-Buckets für allgemeine Zwecke sollten Lifecycle-Konfigurationen haben	AWS Bewährte grundlegende Sicherheitsmethoden, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	NIEDRIG	 Ja	Änderung ausgelöst
S3.14	Für S3-Allzweck-Buckets sollte die Versionierung aktiviert sein	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	NIEDRIG	 Nein	Änderung ausgelöst
S3.15	Bei S3-Allzweck-Buckets sollte Object Lock aktiviert sein	NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MITTEL	 Ja	Änderung ausgelöst
S3.17	S3-Buckets für allgemeine Zwecke sollten im Ruhezustand mit verschlüsselt werden AWS KMS keys	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, durch Service verwalteter Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
S3.19	Bei S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	KRITISCH	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
S3.20	Für S3-Allzweck-Buckets sollte MFA Delete aktiviert sein	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
S3.22	S3-Buckets für allgemeine Zwecke sollten Schreiberereignisse auf Objektebene protokollieren	Benchmark für CIS AWS Foundations v3.0.0, PCI DSS v4.0.1	MITTEL	 Nein	Regelmäßig
S3.23	S3-Buckets für allgemeine Zwecke sollten Leseereignisse auf Objektebene protokollieren	Benchmark für CIS AWS Foundations v3.0.0, PCI DSS v4.0.1	MITTEL	 Nein	Regelmäßig
S3.24	Für S3-Access Points mit mehreren Regionen sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, PCI DSS v4.0.1	HIGH (HOCH)	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
S3.25	S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben	AWS Bewährte grundlegende Sicherheitsmethoden	NIEDRIG	 Ja	Änderung ausgelöst
SageMaker 1.	SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	HIGH (HOCH)	 Nein	Regelmäßig
SageMaker 2.2	SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
SageMaker 3.	Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instanzen haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst
SageMaker 4.	SageMaker Bei Produktionsvarianten für Endgeräte sollte die anfängliche Anzahl der Instanzen größer als 1 sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
SageMaker 5.	SageMaker Modelle sollten eingehenden Verkehr blockieren	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Änderung ausgelöst
SageMaker 6.	SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
SageMaker 7.	SageMaker Bilder sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
SageMaker 8.	SageMaker Notebook-Instanzen sollten auf unterstützten Plattformen laufen	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Regelmäßig
SecretsManager1.	Secrets Manager Manager-Geheimnisse sollte die automatische Rotation aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	MITTEL	 Ja	Änderung ausgelöst
SecretsManager2.2	Secrets Manager Manager-Geheimnisse, die mit automatischer Rotation konfiguriert sind, sollten erfolgreich rotieren	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed-Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
SecretsManager3.	Unbenutzte Secrets Manager Manager-Geheimnisse entfernen	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, Service-Managed Standard: AWS Control Tower	MITTEL	 Ja	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
SecretsManager4.	Secrets Manager Manager-Geheimnisse sollten innerhalb einer bestimmten Anzahl von Tagen rotiert werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	MITTEL	 Ja	Regelmäßig
SecretsManager5.	Secrets Manager Manager-Geheimnisse sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
ServiceCatalog1.	Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Regelmäßig
SES.1	SES-Kontaktlisten sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
SES.2	SES-Konfigurationsätze sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
SNS.1	SNS-Themen sollten im Ruhezustand verschlüsselt werden mit AWS KMS	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MITTEL	 Nein	Änderung ausgelöst
SNS.3	SNS-Themen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
SNS.4	Richtlinien für den Zugriff auf SNS-Themen sollten keinen öffentlichen Zugriff zulassen	AWS Bewährte grundlegende Sicherheitsmethoden	HIGH (HOCH)	 Nein	Änderung ausgelöst
SQS.1	Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
SQS.2	SQS-Warteschlangen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
SQS.3	Die SQS-Richtlinien für den Warteschlangenzugriff sollten keinen öffentlichen Zugriff zulassen	AWS Bewährte grundlegende Sicherheitsmethoden	HIGH (HOCH)	 Nein	Änderung ausgelöst
SSM.1	EC2 Instanzen sollten verwaltet werden von AWS Systems Manager	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, PCI DSS AWS Control Tower v3.2.1, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
SSM.2	EC2 Von Systems Manager verwaltete Instanzen sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	HIGH (HOCH)	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
SSM.3	EC2 Von Systems Manager verwaltete Instanzen sollten den Zuordnungs-Compliance-Status COMPLIANT haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, Service-Managed Standard: AWS Control Tower	NIEDRIG	 Nein	Änderung ausgelöst
SSM.4	SSM-Dokumente sollten nicht öffentlich sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	KRITISCH	 Nein	Regelmäßig
SSM.5	SSM-Dokumente sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
SSM.6	Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
SSM. 7	Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0	KRITISCH	 Nein	Regelmäßig
StepFunctions1.	Step Functions, bei Zustandsmaschinen sollte die Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, PCI DSS v4.0.1	MITTEL	 Ja	Änderung ausgelöst
StepFunctions2.2	Step Functions Functions-Aktivitäten sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
Übertragung.1	Workflows für die Transfer Family sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
Übertragung.2	Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunkterbindung verwenden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Übertragung.3	Bei Connectoren der Transfer Family sollte die Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
Übertragung.4	Transfer Family Familienverträge sollten gekennzeichnet werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
Übertragung.5	Transfer Family Familienzertifikate sollten gekennzeichnet sein	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
Übertragung.6	Steckverbinder der Transfer-Familie sollten gekennzeichnet sein	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
Übertragung.7	Transfer Family Familienprofile sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst
WAF.1	AWS Die WAF Classic Global Web ACL-Protokollierung sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
WAF.2	AWS Die regionalen Regeln von WAF Classic sollten mindestens eine Bedingung enthalten	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
WAF.3	AWS WAF Classic Regional Regelgruppen sollten mindestens eine Regel haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
WAF.4	AWS WAF Classic Regional Web ACLs sollte mindestens eine Regel oder Regelgruppe haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
WAF.6	AWS Globale WAF Classic-Regeln sollten mindestens eine Bedingung haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
WAF.7	AWS Globale WAF Classic-Regelgruppen sollten mindestens eine Regel haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
WAF.8	AWS WAF Classic Global Web ACLs sollte mindestens eine Regel oder Regelgruppe haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
WAF.10	AWS Das WAF-Web ACLs sollte mindestens eine Regel oder Regelgruppe haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
WAF.11	AWS Die WAF-Web-ACL-Protokollierung sollte aktiviert sein	NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	NIEDRIG	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
WAF. 12	AWS Bei WAF-Regeln sollten Metriken aktiviert sein CloudWatch	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MITTEL	 Nein	Änderung ausgelöst
WorkSpaces1.	WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Änderung ausgelöst
WorkSpaces2.2	WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Änderung ausgelöst

Änderungsprotokoll für Security Hub CSPM-Steuerelemente

Im folgenden Änderungsprotokoll werden wesentliche Änderungen an bestehenden AWS Sicherheitskontrollen von Security Hub Cloud Security Posture Management (CSPM) aufgezeichnet, die zu Änderungen des Gesamtstatus einer Kontrolle und des Compliance-Status ihrer Ergebnisse führen können. Informationen darüber, wie Security Hub CSPM den Kontrollstatus bewertet, finden Sie unter: [Bewertung des Konformitätsstatus und des Kontrollstatus](#). Es kann einige Tage nach ihrem Eintrag in diesem Protokoll dauern, bis sich Änderungen auf alle auswirken, AWS-Regionen in denen das Steuerelement verfügbar ist.

In diesem Protokoll werden Änderungen aufgezeichnet, die seit April 2023 vorgenommen wurden. Wählen Sie ein Steuerelement aus, um weitere Informationen dazu einzusehen. Titeländerungen werden 90 Tage lang in der detaillierten Beschreibung eines Steuerelements vermerkt.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
24. Juli 2025	[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	Dieses Steuerelement prüft, ob ein Amazon EKS-Cluster auf einer unterstützten Kubernetes-Version ausgeführt wird. Security Hub CSPM hat den Parameterwert für dieses Steuerelement von 1.30 auf geändert. 1.31 Die Standardunterstützung für Kubernetes Version 1.30 in Amazon EKS endete am 23. Juli 2025.
23. Juli 2025	[EC2.173] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen	Security Hub CSPM hat den Titel dieses Steuerelements geändert. Der neue Titel spiegelt genauer wider, dass das Steuerelement nur Anfragen von Amazon EC2 Spot Fleet überprüft, die Startparameter angeben. Zuvor lautete der Titel dieses Steuerelements: EC2 Spot

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
		Fleet requests should enable encryption for attached EBS volumes.
30. Juni 2025	[IAM.13] Stellen Sie sicher, dass für die IAM-Passwortrichtlinie mindestens ein Symbol erforderlich ist	Security Hub CSPM hat dieses Steuerelement aus dem PCI DSS v4.0.1-Standard entfernt. PCI DSS v4.0.1 verlangt nicht ausdrücklich die Verwendung von Symbolen in Passwörtern.
30. Juni 2025	[IAM.17] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft	Security Hub CSPM hat dieses Steuerelement aus dem Standard NIST SP 800-171 Revision 2 entfernt. NIST SP 800-171 Revision 2 verlangt nicht ausdrücklich, dass Passwörter innerhalb von 90 Tagen oder weniger ablaufen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
30. Juni 2025	[RDS.16] Aurora-DB-Cluster sollten so konfiguriert sein, dass sie Tags in DB-Snapshots kopieren	Security Hub CSPM hat den Titel dieses Steuerelements geändert. Der neue Titel spiegelt genauer wider, dass das Steuerelement nur Amazon Aurora Aurora-DB-Cluster überprüft. Zuvor lautete der Titel dieses Steuerelements: RDS DB clusters should be configured to copy tags to snapshots.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
30. Juni 2025	[SageMaker.8] SageMaker Notebook-Instances sollten auf unterstützten Plattformen laufen	Dieses Steuerelement prüft anhand der für die Notebook-Instance angegebenen Plattform-ID, ob eine Amazon SageMaker AI-Notebook-Instance für die Ausführung auf einer unterstützten Plattform konfiguriert ist. Security Hub CSPM unterstützt notebook-a12-v1 und nicht mehr notebook-a12-v2 als Parameterwerte für dieses Steuerelement. Notebook-Instances, die auf diesen Plattformen laufen, haben am 30. Juni 2025 das Ende des Supports erreicht.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
30. Mai 2025	[IAM.10] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein	Security Hub CSPM hat dieses Steuerelement aus dem PCI DSS v4.0.1-Standard entfernt. Dieses Steuerelement prüft, ob die Kontopasswortrichtlinien für IAM-Benutzer die Mindestanforderungen erfüllen, einschließlich einer Mindestkennwortlänge von 7 Zeichen. PCI DSS v4.0.1 verlangt jetzt, dass Passwörter mindestens 8 Zeichen lang sind. Die Steuerung gilt weiterhin für den Standard PCI DSS v3.2.1, für den andere Kennwortanforderungen gelten. Um die Kennwortrichtlinien für Konten anhand der Anforderungen von PCI DSS v4.0.1 zu bewerten, können Sie das IAM.7-Steuerelement verwenden. Für dieses Steuerelement

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
		müssen Kennwörter mindestens 8 Zeichen lang sein. Es unterstützt auch benutzerdefinierte Werte für die Passwortlänge und andere Parameter. Die IAM.7-Steuerung ist Teil des PCI DSS v4.0.1-Standards in Security Hub CSPM.
8. Mai 2025	[RDS.46] RDS-DB-Instances sollten nicht in öffentlichen Subnetzen mit Routen zu Internet-Gateways bereitgestellt werden	Security Hub CSPM hat die Veröffentlichung des Steuerelements RDS.46 insgesamt rückgängig gemacht. AWS-Regionen Bisher unterstützte dieses Steuerelement den FSBP-Standard (AWS Foundational Security Best Practices).

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
7. April 2025	[ELB.17] Anwendungs- und Netzwerk-Load-Balancer mit Listnern sollten die empfohlenen Sicherheitsrichtlinien verwenden	Dieses Steuerelement prüft, ob der HTTPS-Listener für einen Application Load Balancer oder der TLS-Listener für einen Network Load Balancer so konfiguriert ist, dass Daten während der Übertragung mithilfe einer empfohlenen Sicherheitsrichtlinie nie verschlüsselt werden. Security Hub CSPM unterstützt jetzt zwei zusätzliche Parameterwerte für dieses Steuerelement: ELBSecurityPolicy-TLS13-1-2-Res-2021-06 und ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
27. März 2025	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Dieses Steuerelement überprüft, ob die Laufzeiteinstellungen für eine AWS Lambda Funktion den erwarteten Werten für unterstützte Laufzeiten in jeder Sprache entsprechen. Security Hub CSPM unterstützt dieses Steuerelement jetzt <code>ruby3.4</code> als Parameterwert. AWS Lambda Unterstützung für diese Laufzeit hinzugefügt.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
26. März 2025	[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	Dieses Steuerelement prüft, ob ein Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster auf einer unterstützten Kubernetes-Version ausgeführt wird. Für den <code>oldestVersionSupported</code> Parameter hat Security Hub CSPM den Wert von <code>1.29</code> auf geändert. <code>1.30</code> Die älteste unterstützte Kubernetes-Version ist jetzt verfügbar. <code>1.30</code>

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
10. März 2025	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Dieses Steuerelement überprüft, ob die Laufzeiteinstellungen für eine AWS Lambda Funktion den erwarteten Werten für unterstützte Laufzeiten in jeder Sprache entsprechen. Security Hub CSPM unterstützt dotnet6 und nicht mehr python3.8 als Parameterwerte für dieses Steuerelement. AWS Lambda unterstützt diese Laufzeiten nicht mehr.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
7. März 2025	[RDS.18] RDS-Instances sollten in einer VPC bereitgestellt werden	Security Hub CSPM hat dieses Steuerelement aus dem Standard „Best Practices für AWS grundlegende Sicherheit“ entfernt und die Überprüfung der Anforderungen von NIST SP 800-53 Rev. 5 automatisiert. Da Amazon EC2 -Classic Networking eingestellt wurde, können Amazon Relational Database Service (Amazon RDS) - Instances nicht mehr außerhalb einer VPC bereitgestellt werden. Die Steuerung ist weiterhin Teil des Service-Managed-Standards.AWS Control Tower
10. Januar 2025	[Glue.2] Bei AWS Glue-Jobs sollte die Protokollierung aktiviert sein	Security Hub CSPM hat dieses Steuerelement entfernt und es aus allen Standards entfernt.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
20. Dezember 2024	EC26.1 bis 1.69 EC2	Security Hub CSPM hat die Version der Steuerelemente EC2 6.1 bis EC2 1.69 rückgängig gemacht.
12. Dezember 2024	[RDS.23] RDS-Instances sollten keinen Standard-Port für die Datenbank-Engine verwenden	RDS.23 prüft, ob ein Amazon Relational Database Service (Amazon RDS) - Cluster oder eine Instance einen anderen Port als den Standardport der Datenbank-Engine verwendet. Wir haben das Steuerelement aktualisiert, sodass die zugrunde liegende AWS Config Regel das Ergebnis von NOT_APPLICABLE für RDS-Instances zurückgibt, die Teil eines Clusters sind.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
2. Dezember 2024	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub CSPM unterstützt jetzt <code>nodejs22.x</code> als Parameter.
26. November 2024	[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	Dieses Steuerelement prüft, ob ein Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster auf einer unterstützten Kubernetes-Version ausgeführt wird. Die älteste unterstützte Version ist jetzt 1.29

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
20. November 2024	[Config.1] AWS Config sollte aktiviert sein und die serviceverknüpfte Rolle für die Ressourcenaufzeichnung verwenden	Config.1 prüft, ob aktiviert AWS Config ist, verwendet die serviceverknüpfte Rolle und zeichnet Ressourcen für aktivierte Steuerelemente auf. Security Hub CSPM erhöhte den Schweregrad dieser Kontrolle von MEDIUM auf. CRITICAL Security Hub CSPM fügte außerdem neue Statuscodes und Statusgründe für fehlgeschlagene Config.1-Ergebnisse hinzu. Diese Änderungen spiegeln die Bedeutung von Config.1 für den Betrieb der Security Hub CSPM-Steuerelemente wider. Wenn Sie die Aufzeichnung von Ressourcen deaktiviert haben AWS Config, kann es sein, dass Sie falsche Kontrolleergebnisse erhalten.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
		Um ein PASSED Ergebnis für Config.1 zu erhalten, aktivieren Sie die Ressourcen aufzeichnung für Ressourcen, die den aktivierten Security Hub CSPM-Steurelementen entsprechen, und deaktivieren Sie Kontrollen, die in Ihrer Organisation nicht erforderlich sind. Anweisungen zur Konfiguration AWS Config für Security Hub CSPM finden Sie unter. Aktivierung und Konfiguration AWS Config für Security Hub CSPM Eine Liste der Security Hub CSPM-Steurelemente und der entsprechenden Ressourcen finden Sie unter. Erforderliche AWS Config Ressourcen für Kontrollbefunde

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. November 2024	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub CSPM unterstützt jetzt python3.13 als Parameter.
11. Oktober 2024	ElastiCache steuert	Die Titel der Steuerelemente für ElastiCache .3, ElastiCache .4, ElastiCache .5 und ElastiCache .7 wurden geändert. In den Titeln wird Redis OSS nicht mehr erwähnt, da die Steuerelemente auch für Valkey gelten. ElastiCache

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
27. September 2024	[ELB.4] Application Load Balancer sollte so konfiguriert sein, dass ungültige HTTP-Header gelöscht werden	Der geänderte Titel des Steuerelements von Application Load Balancer sollte so konfiguriert werden, dass HTTP-Header gelöscht werden. Application Load Balancer sollte so konfiguriert sein, dass ungültige HTTP-Header gelöscht werden.
19. August 2024	Der Titel ändert sich zu DMS.12 und zu den Steuerelementen ElastiCache	Die Titel der Steuerelemente für DMS.12 und ElastiCache DMS.1 bis 1.7 wurden geändert. ElastiCache Wir haben diese Titel geändert, um einer Namensänderung im Service Amazon ElastiCache (Redis OSS) Rechnung zu tragen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
15. August 2024	[Config.1] AWS Config sollte aktiviert sein und die serviceverknüpfte Rolle für die Ressourcenaufzeichnung verwenden	Config.1 prüft, ob aktiviert AWS Config ist, verwendet die serviceverknüpfte Rolle und zeichnet Ressourcen für aktivierte Steuerelemente auf. Security Hub CSPM hat einen benutzerdefinierten Steuerparameter mit dem Namen hinzugefügt. <code>includeConfigServiceLinkedRoleCheck</code> Wenn Sie diesen Parameter auf <code>false</code> setzen, können Sie sich von der Überprüfung abmelden, ob die serviceverknüpfte AWS Config Rolle verwendet wird.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
31. Juli 2024	[IoT.1] AWS IoT Device Defender Sicherheitsprofile sollten markiert werden	Der Titel des Steuerelements wurde von AWS IoT Core Sicherheitsprofilen sollte markiert werden zu AWS IoT Device Defender Sicherheitsprofile sollten markiert werden geändert.
29. Juli 2024	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub CSPM unterstützt nicht mehr <code>nodejs16.x</code> als Parameter.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
29. Juli 2024	[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	Dieses Steuerelement prüft, ob ein Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster auf einer unterstützten Kubernetes-Version ausgeführt wird. Die älteste unterstützte Version ist. 1.28
25. Juni 2024	[Config.1] AWS Config sollte aktiviert sein und die serviceverknüpfte Rolle für die Ressourcenaufzeichnung verwenden	Dieses Steuerelement überprüft, ob AWS Config es aktiviert ist, verwendet die dienstverknüpfte Rolle und zeichnet Ressourcen für aktivierte Steuerelemente auf. Security Hub CSPM hat den Titel der Kontrolle aktualisiert, um widerzuspiegeln, was die Kontrolle bewertet.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
14. Juni 2024	[RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch	Diese Steuerung prüft, ob ein Amazon Aurora MySQL-DB-Cluster so konfiguriert ist, dass er Audit-Logs in Amazon CloudWatch Logs veröffentlicht. Security Hub CSPM hat das Steuerelement aktualisiert, sodass es keine Ergebnisse für Aurora Serverless v1-DB-Cluster generiert.
11. Juni 2024	[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	Dieses Steuerelement prüft, ob ein Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster auf einer unterstützten Kubernetes-Version ausgeführt wird. Die älteste unterstützte Version ist. 1.27

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
10. Juni 2024	[Config.1] AWS Config sollte aktiviert sein und die serviceverknüpfte Rolle für die Ressourcenaufzeichnung verwenden	Dieses Steuerelement überprüft, ob aktiviert AWS Config ist und ob die AWS Config Ressourcenaufzeichnung aktiviert ist. Bisher führte das Steuerelement nur dann PASSED zu einem Ergebnis, wenn Sie die Aufzeichnung für alle Ressourcen konfiguriert hatten. Security Hub CSPM hat das Steuerelement aktualisiert, sodass ein PASSED Ergebnis angezeigt wird, wenn die Aufzeichnung für Ressourcen aktiviert ist, die für aktivierte Steuerungen erforderlich sind. Das Steuerelement wurde außerdem aktualisiert, um zu überprüfen, ob die AWS Config dienstbezogene Rolle verwendet wird, die Berechtigungen zum Aufzeichnen der erforderlichen

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
		Ressourcen bereitgestellt.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
8. Mai 2024	[S3.20] Bei S3-Allzweck-Buckets sollte MFA Delete aktiviert sein	Dieses Steuerelement prüft, ob bei einem versionsbasierten Amazon S3-Bucket für allgemeine Zwecke das Löschen mit Multi-Faktor-Authentifizierung (MFA) aktiviert ist. Zuvor ergab die Kontrolle einen FAILED Befund für Buckets, die über eine Lifecycle-Konfiguration verfügen. Das Löschen von MFA mit Versionierung kann jedoch nicht für einen Bucket aktiviert werden, der über eine Lifecycle-Konfiguration verfügt. Security Hub CSPM hat die Steuerung aktualisiert, sodass keine Ergebnisse für Buckets mit einer Lifecycle-Konfiguration vorliegen. Die Beschreibung des Steuerelements wurde aktualisiert, um

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
		das aktuelle Verhalten widerzuspiegeln.
2. Mai 2024	[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	Security Hub CSPM hat die älteste unterstützte Version von Kubernetes, auf der der Amazon EKS-Cluster ausgeführt werden kann, aktualisiert, um ein bestehendes Ergebnis zu erzielen. Die derzeit älteste unterstützte Version ist Kubernetes 1.26

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
30. April 2024	[CloudTrail.3] Mindestens ein CloudTrail Trail sollte aktiviert sein	Der Titel des Steuerelements wurde von „CloudTrail sollte aktiviert“ auf „Mindestens ein CloudTrail Trail sollte aktiviert sein“ geändert. Dieses Steuerelement zeigt derzeit PASSED an AWS-Konto , ob für mindestens ein CloudTrail Trail aktiviert ist. Der Titel und die Beschreibung wurden geändert, um das aktuelle Verhalten genau widerzuspiegeln.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
29. April 2024	[AutoScaling.1] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden	Der Titel der Steuerung wurde von Auto Scaling Scaling-Gruppen, die einem Classic Load Balancer zugeordnet sind, sollten Load Balancer-Integritätsprüfungen verwenden, zu Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, ELB-Zustandsprüfungen verwenden. Dieses Steuerelement bewertet derzeit Anwendungs-, Gateway-, Netzwerk- und Classic Load Balancer. Der Titel und die Beschreibung wurden geändert, um das aktuelle Verhalten genau widerzuspiegeln.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
19. April 2024	[CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst	Das Steuerelement überprüft, ob AWS CloudTrail es aktiviert und mit mindestens einem Multiregionspfad konfiguriert ist, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst. Bisher generierte das Steuerelement fälschlicherweise PASSED Ergebnisse, wenn ein Konto mit mindestens einem Multiregions-Trail CloudTrail aktiviert und konfiguriert war, auch wenn kein Trail Lese- und Schreibverwaltungsereignisse aufzeichnete. Das Steuerelement generiert jetzt nur noch PASSED Ergebnisse, wenn CloudTrail es aktiviert und mit mindestens einem multiregionalen Trail konfiguriert ist, der Verwaltungsereignisse für Lese-

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
		und Schreibvorgänge erfasst.
10. April 2024	[Athena.1] Athena-Arbeitsgruppen sollten im Ruhezustand verschlüsselt werden	Security Hub CSPM hat dieses Steuerelement entfernt und es aus allen Standards entfernt. Athena-Arbeitsgruppen senden Protokolle an Amazon Simple Storage Service (Amazon S3)-Buckets. Amazon S3 bietet jetzt Standardverschlüsselung mit S3-verwalteten Schlüsseln (SS3-S3) für neue und bestehende S3-Buckets.
10. April 2024	[AutoScaling.4] Die Auto Scaling Scaling-Gruppenstartkonfiguration sollte kein Metadaten-Response-Hop-Limit größer als 1 haben	Security Hub CSPM hat dieses Steuerelement entfernt und es aus allen Standards entfernt. Die Limits für Metadaten-Antwort-Hops für Amazon Elastic Compute Cloud (Amazon EC2)-Instances hängen von der Arbeitslast ab.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
10. April 2024	[CloudFormation.1] CloudFormation Stacks sollten in Simple Notification Service (SNS) integriert werden	Security Hub CSPM hat dieses Steuerelement entfernt und es aus allen Standards entfernt. Die Integration von AWS CloudFormation Stacks mit Amazon SNS SNS-Themen ist keine bewährte Sicherheitsmethode mehr. Die Integration wichtiger CloudFormation Stacks mit SNS-Themen kann zwar nützlich sein, ist aber nicht für alle Stacks erforderlich.
10. April 2024	[CodeBuild.5] In CodeBuild Projektum gebungen sollte der privilegierte Modus nicht aktiviert sein	Security Hub CSPM hat dieses Steuerelement entfernt und es aus allen Standards entfernt. Die Aktivierung des privilegierten Modus in einem CodeBuild Projekt stellt kein zusätzliches Risiko für die Kundenumgebung dar.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
10. April 2024	[IAM.20] Vermeiden Sie die Verwendung des Root-Benutzers	Security Hub CSPM hat dieses Steuerelement entfernt und es aus allen Standards entfernt. Der Zweck dieser Kontrolle wird durch eine andere Kontrolle abgedeckt ,. [CloudWatch.1] Für den Benutzer „root“ sollten ein Filter und ein Alarm für die Log-Metrik vorhanden sein
10. April 2024	[SNS.2] Die Protokollierung des Zustellungsstatus sollte für Benachrichtigungen, die an ein Thema gesendet werden, aktiviert sein	Security Hub CSPM hat dieses Steuerelement entfernt und es aus allen Standards entfernt. Das Protokollieren des Zustellungsstatus für SNS-Themen ist keine bewährte Sicherheitmethode mehr. Das Protokollieren des Zustellungsstatus für wichtige SNS-Themen kann zwar nützlich sein, ist aber nicht für alle Themen erforderlich.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
10. April 2024	[S3.10] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben	Security Hub CSPM hat dieses Steuerelement aus AWS Foundational Security Best Practices und Service-Managed Standard entfernt: . AWS Control Tower Der Zweck dieser Kontrolle wird durch zwei weitere Steuerelemente abgedeckt: und. [S3.13] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben [S3.14] Für S3-Allzweck-Buckets sollte die Versionierung aktiviert sein Diese Steuerung ist immer noch Teil von NIST SP 800-53 Rev. 5.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
10. April 2024	[S3.11] Bei S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein	Security Hub CSPM hat dieses Steuerelement aus AWS Foundational Security Best Practices und Service-Managed Standard entfernt:. AWS Control Tower Es gibt zwar einige Fälle, in denen Ereignisbenachrichtigungen für S3-Buckets nützlich sind, dies ist jedoch keine allgemein anerkannte bewährte Sicherheitmethode. Diese Steuerung ist immer noch Teil von NIST SP 800-53 Rev. 5.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
10. April 2024	[SNS.1] SNS-Themen sollten im Ruhezustand wie folgt verschlüsselt werden AWS KMS	Security Hub CSPM hat dieses Steuerelement aus AWS Foundational Security Best Practices und Service-Managed Standard entfernt:. AWS Control Tower Standardmäßig verschlüsselt SNS ruhende Themen mit Festplattenverschlüsselung. Weitere Informationen finden Sie unter Datenverschlüsselung . Die Verwendung AWS KMS zur Verschlüsselung von Themen wird als bewährte Sicherheitsmethode nicht mehr empfohlen. Dieses Steuerelement ist immer noch Teil von NIST SP 800-53 Rev. 5.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
8. April 2024	[ELB.6] Für Anwendungen, Gateways und Network Load Balancers sollte der Löschschutz aktiviert sein	Der Steuerelementtitel wurde von Application Load Balancer Balancer-Löschschutz aktiviert in Application, Gateway und Network Load Balancer sollten den Löschschutz aktiviert haben geändert. Dieses Steuerelement bewertet derzeit Application, Gateway und Network Load Balancer. Der Titel und die Beschreibung wurden geändert, um das aktuelle Verhalten genau widerzuspiegeln.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
22. März 2024	[Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden	Der Titel des Steuerelements wurde von Verbindungen zu OpenSearch Domänen sollten mit TLS 1.2 verschlüsselt werden in Verbindungen zu OpenSearch Domänen sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden geändert. Bisher überprüfte das Steuerelement nur, ob Verbindungen zu OpenSearch Domänen TLS 1.2 verwendeten. Das Steuerelement stellt nun PASSED fest, ob OpenSearch Domänen mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt wurden. Der Titel und die Beschreibung des Steuerelements wurden aktualisiert, um das aktuelle Verhalten widerzuspiegeln.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
22. März 2024	[ES.8] Verbindungen zu Elasticsearch-Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden	Der Titel des Steuerelements wurde von <code>Connections zu Elasticsearch-Domains geändert</code> und sollte mit TLS 1.2 verschlüsselt werden. Verbindungen zu Elasticsearch-Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden. Bisher überprüfte das Steuerelement nur, ob Verbindungen zu Elasticsearch-Domains TLS 1.2 verwendeten. Das Steuerelement stellt nun PASSED fest, ob Elasticsearch-Domains mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt wurden. Der Titel und die Beschreibung des Steuerelements wurden aktualisiert, um das aktuelle Verhalten widerzuspiegeln.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. März 2024	[S3.1] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein	Der Titel sollte von der Einstellung „Öffentlichen Zugriff blockieren“ auf die Einstellung „Öffentlichen Zugriff blockieren“ in S3-Allzweck-Buckets geändert werden. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.
12. März 2024	[S3.2] S3-Allzweck-Buckets sollten den öffentlichen Lesezugriff blockieren	Der geänderte Titel von S3-Buckets sollte den öffentlichen Lesezugriff auf S3-Buckets verbieten. Allzweck-Buckets sollten den öffentlichen Lesezugriff blockieren. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. März 2024	[S3.3] S3-Allzweck-Buckets sollten den öffentlichen Schreibzugriff blockieren	Der geänderte Titel von S3-Buckets sollte den öffentlichen Schreibzugriff auf S3-Buckets verbieten . Allzweck-Buckets sollten den öffentlichen Schreibzugriff blockieren. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.
12. März 2024	[S3.5] S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erfordern	Die Änderung des Titels von S3-Buckets sollte Anfragen zur Verwendung von Secure Socket Layer erfordern, zu S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erfordern. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. März 2024	[S3.6] Allgemeine S3-Bucket-Richtlinien sollten den Zugriff auf andere einschränken AWS-Konten	Der geänderte Titel von S3-Berechtigungen, die anderen AWS-Konten in Bucket-Richtlinien gewährt wurden, sollte auf S3-Allzweck-Bucket-Richtlinien beschränkt werden, sollten den Zugriff auf andere einschränken AWS-Konten. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.
12. März 2024	[S3.7] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden	Bei der Änderung des Titels von S3-Buckets sollte die regionsübergreifende Replikation aktiviert sein, sodass für S3-Buckets für allgemeine Zwecke die regionsübergreifende Replikation verwendet werden sollte. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. März 2024	[S3.7] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden	Bei der Änderung des Titels von S3-Bucket s sollte die regionsübergreifende Replikation aktiviert sein, sodass für S3-Bucket s für allgemeine Zwecke die regionsübergreifende Replikation verwendet werden sollte. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.
12. März 2024	[S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren	Der Titel sollte von der Einstellung „Öffentlichen Zugriff blockieren“ auf Bucket-Ebene in die Einstellung für S3-Allzweck-Bucket s geändert werden, die den öffentlichen Zugriff blockieren sollen. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. März 2024	[S3.9] Bei S3-Allzweck-Buckets sollte die Serverzugriffsprotokollierung aktiviert sein	Der Titel wurde von der Protokollierung des S3-Bucket-Serverzugriffs aktiviert in die Serverzugriffsprotokollierung sollte für S3-Allzweck-Buckets aktiviert sein geändert. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.
12. März 2024	[S3.10] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben	Bei der Änderung des Titels von S3-Buckets mit aktivierter Versionierung sollten Lebenszyklusrichtlinien so konfiguriert sein, dass S3-Allzweck-Buckets mit aktivierter Versionierung Lifecycle-Konfigurationen haben sollten. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. März 2024	[S3.11] Bei S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein	Bei der Änderung des Titels von S3-Bucket s sollten Ereignisbenachrichtigungen aktiviert sein, bei S3-Buckets für allgemeine Zwecke sollten Ereignisbenachrichtigungen aktiviert sein. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.
12. März 2024	[S3.12] ACLs sollte nicht zur Verwaltung des Benutzerzugriffs auf S3-Allzweck-Buckets verwendet werden	Der geänderte Titel aus den S3-Zugriffskontrolllisten (ACLs) sollte nicht zur Verwaltung des Benutzerzugriffs auf Buckets verwendet werden. Er ACLs sollte auch nicht zur Verwaltung des Benutzerzugriffs auf S3-Allzweck-Buckets verwendet werden. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. März 2024	[S3.13] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben	Bei der Änderung des Titels von S3-Buckets sollten die Lebenszyklusrichtlinien so konfiguriert sein, dass S3-Allzweck-Buckets Lifecycle-Konfigurationen haben sollten. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.
12. März 2024	[S3.14] Für S3-Allzweck-Buckets sollte die Versionierung aktiviert sein	Bei der Änderung des Titels von S3-Buckets sollte Versionierung verwendet werden, bei S3-Buckets für allgemeine Zwecke sollte die Versionierung aktiviert sein. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. März 2024	[S3.15] Bei S3-Allzweck-Buckets sollte Object Lock aktiviert sein	Der geänderte Titel von S3-Buckets sollte so konfiguriert werden, dass Object Lock verwendet wird. Für S3-Allzweck-Buckets sollte Object Lock aktiviert sein. Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.
12. März 2024	[S3.17] S3-Allzweck-Buckets sollten im Ruhezustand verschlüsselt werden mit AWS KMS keys	Der Titel wurde von S3-Buckets sollten im Ruhezustand mit AWS KMS keys verschlüsselt werden in S3-Buckets für allgemeine Zwecke geändert. AWS KMS keys Security Hub CSPM hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
7. März 2024	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub CSPM unterstützt jetzt <code>nodejs20.x</code> und <code>ruby3.3</code> als Parameter.
22. Februar 2024	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub CSPM unterstützt jetzt <code>dotnet8</code> als Parameter.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
5. Februar 2024	[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	Security Hub CSPM hat die älteste unterstützte Version von Kubernetes, auf der der Amazon EKS-Cluster ausgeführt werden kann, aktualisiert, um ein bestehendes Ergebnis zu erzielen. Die derzeit älteste unterstützte Version ist Kubernetes 1.25

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
10. Januar 2024	[CodeBuild.1] Das CodeBuild Bitbucket-Quell-Repository URLs sollte keine vertraulichen Anmeldeinformationen enthalten	Der geänderte Titel CodeBuild GitHub oder das Bitbucket -Quell-Repository URLs sollte in das CodeBuild Bitbucket -Quell-Repository geändert werden und URLs darf keine vertraulichen Anmeldeinformationen enthalten. OAuth Security Hub CSPM hat die Erwähnung davon entfernt OAuth , da auch andere Verbindungsmethoden sicher sein können. Security Hub CSPM hat die Erwähnung davon entfernt GitHub, da es nicht mehr möglich ist, ein persönliches Zugriffstoken oder einen Benutzernamen und ein Passwort im GitHub Quell-Repository zu haben. URLs

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
8. Januar 2024	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub CSPM unterstützt go1.x und nicht mehr java8 als Parameter, da es sich dabei um ausgemusterte Laufzeiten handelt.
29. Dezember 2023	[RDS.8] Für RDS-DB-Instances sollte der Löschschutz aktiviert sein	RDS.8 prüft, ob für eine Amazon RDS-DB-Instance, die eine der unterstützten Datenbank-Engines verwendet, der Löschschutz aktiviert ist. Security Hub CSPM unterstützt jetzt custom-oracle-eeoracle-ee-cdb, und oracle-se2-cdb als Datenbank-Engines.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
22. Dezember 2023	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub CSPM unterstützt jetzt <code>java21</code> und <code>python3.12</code> als Parameter. Security Hub CSPM unterstützt nicht mehr <code>ruby2.7</code> als Parameter.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
15. Dezember 2023	Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein	CloudFront.1 prüft, ob für eine CloudFront Amazon-Distribution ein Standard-Root-Objekt konfiguriert ist. Security Hub CSPM hat den Schweregrad dieser Kontrolle von CRITICAL auf HIGH herabgesetzt, da das Hinzufügen des Standard-Root-Objekts eine Empfehlung ist, die von der Anwendung und den spezifischen Anforderungen des Benutzers abhängt.
05. Dezember 2023	[EC2.13] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen	Der Titel des Steuerelements wurde von Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 auf Port 22 zulassen in Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 oder: :/0 auf Port 22 zulassen geändert.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
05. Dezember 2023	[EC2.14] Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 oder: :/0 auf Port 3389 zulassen	Der Kontrolltitel wurde von „Sicherstellen, dass keine Sicherheitsgruppen den Zugriff von 0.0.0.0/0 auf Port 3389 zulassen“ in „Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 oder: :/0 auf Port 3389 zulassen“ geändert.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
05. Dezember 2023	[RDS.9] RDS-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch	Der Kontrolltitel wurde von Datenbank protokollierung sollte aktiviert sein in RDS-DB-Instances geändert, sodass RDS-DB-Instances Protokolle in Logs veröffentlichen sollten. CloudWatch Security Hub CSPM hat festgestellt, dass dieses Steuerelement nur prüft, ob Protokolle in Amazon CloudWatch Logs veröffentlicht werden, und nicht, ob RDS-Protokolle aktiviert sind. Die Steuerung stellt PASSED fest, ob RDS-DB-Instances so konfiguriert sind, dass sie Protokolle in Logs veröffentlichen. CloudWatch Der Titel des Steuerelements wurde aktualisiert, um das aktuelle Verhalten widerzuspiegeln.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
05. Dezember 2023	[EKS.8] Bei EKS-Clustern sollte die Auditprotokollierung aktiviert sein	Diese Steuerung prüft, ob bei Amazon EKS-Clustern die Auditprotokollierung aktiviert ist. Die AWS Config Regel, die Security Hub CSPM zur Auswertung dieser Kontrolle verwendet, wurde von eks-cluster-logging-enabled zu eks-cluster-log-enabled geändert.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
17. November 2023	[EC2.19] Sicherheitsgruppen sollten keinen uneingeschränkten Zugriff auf Ports mit hohem Risiko zulassen	EC2.19 prüft, ob uneingeschränkter eingehender Datenverkehr für eine Sicherheitsgruppe über die angegebenen Ports zugänglich ist, die als risikoreich eingestuft werden. Security Hub CSPM hat dieses Steuerelement aktualisiert, um verwaltete Präfixlisten zu berücksichtigen, wenn sie als Quelle für eine Sicherheitsgruppenregel bereitgestellt werden. Das Steuerelement ermittelt, ob die Präfixlisten die Zeichenketten '0.0.0.0/0' oder ':::/0' enthalten. FAILED

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
16. November 2023	[CloudWatch.15] Für CloudWatch Alarme sollten bestimmte Aktionen konfiguriert sein	Der Titel des Steuerelements wurde von „CloudWatch Alarme sollte eine Aktion für den ALARM-Status konfigurieren“ zu „CloudWatch Alarme sollten bestimmte Aktionen konfiguriert haben“ geändert.
16. November 2023	[CloudWatch.16] CloudWatch Protokollgruppen sollten für einen bestimmten Zeitraum aufbewahrt werden	Der geänderte Kontrolltitel aus CloudWatch Protokollgruppen sollte mindestens ein Jahr lang aufbewahrt werden, während CloudWatch Protokollgruppen für einen bestimmten Zeitraum aufbewahrt werden sollten.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
16. November 2023	[Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren	Der Titel der Steuerung wurde von VPC-Lambda-Funktionen sollten in mehr als einer Availability Zone funktionieren, in VPC-Lambda-Funktionen geändert, die in mehreren Availability Zones funktionieren sollten.
16. November 2023	[AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben	Der Titel des Steuerelements wurde von AWS AppSync sollte die Protokollierung auf Anfrage- und Feldebene aktiviert haben in Die Protokollierung auf Feldebene sollte aktiviert sein geändert.AWS AppSync

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
16. November 2023	[EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben	Der Kontrolltitel wurde von Amazon Elastic MapReduce Cluster-Masterknoten sollten keine öffentlichen IP-Adressen haben zu Amazon EMR-Cluster-Primärknoten sollten keine öffentlichen IP-Adressen haben.
16. November 2023	[Opensearch.2] OpenSearch -Domains sollten nicht öffentlich zugänglich sein	Der Titel der Steuerung wurde von OpenSearch Domänen, die sich in einer VPC befinden sollten, zu OpenSearch Domänen geändert, die nicht öffentlich zugänglich sein sollten.
16. November 2023	[ES.2] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein	Der Titel des Steuerelements wurde von Elasticsearch-Domains in einer VPC geändert und Elasticsearch-Domains sollten nicht öffentlich zugänglich sein.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
31. Oktober 2023	[ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein	ES.4 prüft, ob Elasticsearch-Domains so konfiguriert sind, dass sie Fehlerprotokolle an Amazon CloudWatch Logs senden. Die Kontrolle ergab zuvor einen PASSED Befund für eine Elasticsearch-Domain, deren Logs so konfiguriert sind, dass sie an Logs gesendet werden. CloudWatch Security Hub CSPM hat das Steuerelement aktualisiert, sodass nur ein PASSED Ergebnis für eine Elasticsearch-Domain generiert wird, die so konfiguriert ist, dass sie Fehlerprotokolle an Logs sendet. CloudWatch Das Steuerelement wurde außerdem aktualisiert, um Elasticsearch-Versionen, die Fehlerprotokolle nicht unterstützen,

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
		von der Auswertung auszuschließen.
16. Oktober 2023	[EC2.13] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen	EC2.13 prüft, ob Sicherheitsgruppen uneingeschränkten Eingangszugriff auf Port 22 zulassen. Security Hub CSPM hat dieses Steuerelement aktualisiert, um verwaltete Präfixlisten zu berücksichtigen, wenn sie als Quelle für eine Sicherheitsgruppenregel bereitgestellt werden. Das Steuerelement ermittelt, ob die Präfixlisten die Zeichenketten '0.0.0.0/0' oder ': :/0' enthalten. FAILED

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
16. Oktober 2023	[EC2.14] Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 oder: :/0 auf Port 3389 zulassen	EC2.14 überprüft, ob Sicherheitsgruppen uneingeschränkten Zugriff auf Port 3389 zulassen. Security Hub CSPM hat dieses Steuerelement aktualisiert, um verwaltete Präfixlisten zu berücksichtigen, wenn sie als Quelle für eine Sicherheitsgruppenregel bereitgestellt werden. Das Steuerelement ermittelt, ob die Präfixlisten die Zeichenketten '0.0.0.0/0' oder ': :/0' enthalten. FAILED

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
16. Oktober 2023	[EC2.18] Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Datenverkehr für autorisierte Ports zulassen	EC2.18 überprüft, ob die verwendeten Sicherheitsgruppen uneingeschränkten eingehenden Datenverkehr zulassen. Security Hub CSPM hat dieses Steuerelement aktualisiert, um verwaltete Präfixlisten zu berücksichtigen, wenn sie als Quelle für eine Sicherheitsgruppenregel bereitgestellt werden. Das Steuerelement ermittelt, ob die Präfixlisten die Zeichenketten '0.0.0.0/0' oder ':::/0' enthalten. FAILED

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
16. Oktober 2023	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub CSPM unterstützt jetzt <code>python3.11</code> als Parameter.
04. Oktober 2023	[S3.7] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden	Security Hub CSPM hat den Parameter <code>ReplicationType</code> mit dem Wert <code>CROSS-REGION</code> hinzugefügt, um sicherzustellen, dass bei S3-Buckets die regionsübergreifende Replikation aktiviert ist und nicht die Replikation derselben Region.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
27. September 2023	[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	Security Hub CSPM hat die älteste unterstützte Version von Kubernetes, auf der der Amazon EKS-Cluster ausgeführt werden kann, aktualisiert, um ein bestehendes Ergebnis zu erzielen. Die derzeit älteste unterstützte Version ist Kubernetes 1.24

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
20. September 2023	[CloudFront.2] Bei CloudFront Distributionen sollte die Origin-Zugriffsidentität aktiviert sein	Security Hub CSPM hat dieses Steuerelement entfernt und es aus allen Standards entfernt. Folgen Sie stattdessen der Anleitung unter [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden . Die Zugriffskontrolle von Origin ist derzeit die bewährte Methode im Bereich Sicherheit. Diese Kontrolle wird in 90 Tagen aus der Dokumentation entfernt.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
20. September 2023	[EC2.22] Ungenutzte EC2 Amazon-Sicherheitsgruppen sollten entfernt werden	Security Hub CSPM hat dieses Steuerelement aus AWS Foundational Security Best Practices (FSBP) und SP 800-53 Rev. 5 des National Institute of Standards and Technology (NIST) entfernt. Es ist immer noch Teil des Service-Managed Standard: AWS Control Tower. Dieses Steuerelement führt zu einer bestandenen Feststellung, ob Sicherheitsgruppen an EC2 Instances oder an eine elastic network interface angehängt sind. In bestimmten Anwendungsfällen stellen nicht verknüpfte Sicherheitsgruppen jedoch kein Sicherheitsrisiko dar. Sie können andere EC2 Steuerelemente wie EC2 .2, EC2 .13, EC2 .14, EC2 .18 und .19 verwenden, um Ihre

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
		Sicherheitsgruppen zu überwachen. EC2
20. September 2023	[EC2.29] EC2 Instances sollten in einer VPC gestartet werden	Security Hub CSPM hat dieses Steuerelement entfernt und es aus allen Standards entfernt. Amazon EC2 hat EC2 -Classic-Instances zu einer VPC migriert. Dieses Steuerelement wird in 90 Tagen aus der Dokumentation entfernt.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
20. September 2023	[S3.4] Für S3-Buckets sollte die serverseitige Verschlüsselung aktiviert sein.	Security Hub CSPM hat dieses Steuerelement entfernt und es aus allen Standards entfernt. Amazon S3 bietet jetzt Standardverschlüsselung mit S3-verwalteten Schlüsseln (SS3-S3) für neue und bestehende S3-Buckets. Die Verschlüsselungseinstellungen für bestehende Buckets, die mit der serverseitigen Verschlüsselung SS3 -S3 oder SS3 -KMS verschlüsselt sind, bleiben unverändert. Dieses Steuerelement wird in 90 Tagen aus der Dokumentation entfernt.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
14. September 2023	[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen	Der Titel des Steuerelements wurde von Die VPC-Standardsicherheitsgruppe sollte keinen eingehenden und ausgehenden Datenverkehr zulassen zu VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen geändert.
14. September 2023	[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein	Der Steuertitel wurde von Virtual MFA sollte für den Root-Benutzer aktiviert sein zu MFA sollte für den Root-Benutzer aktiviert sein geändert.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
14. September 2023	[RDS.19] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Cluster-Ereignisse konfiguriert werden	Der Titel des Steuerelements wurde von Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Clusterereignisse konfiguriert werden in Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Clusterereignisse konfiguriert werden geändert.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
14. September 2023	[RDS.20] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Ereignisse der Datenbankinstanz konfiguriert werden	Der Titel des Steuerelements wurde von Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbank instanzereignisse konfiguriert werden in Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Datenbank instanzereignisse konfiguriert werden geändert.
14. September 2023	[WAF.2] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung haben	Der Kontrolltitel wurde von „Eine WAF-Regionalregel sollte mindestens eine Bedingung haben“ in „AWS WAF Klassische Regionalregeln“ geändert, die mindestens eine Bedingung haben sollten.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
14. September 2023	[WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben	Der Kontrolltitel wurde von einer regionalen WAF-Regelgruppe mit mindestens einer Regel zu einer AWS WAF klassischen regionalen Regelgruppe geändert. Regelgruppen sollten mindestens eine Regel haben.
14. September 2023	[WAF.4] AWS WAF Classic Regional Web ACLs sollte mindestens eine Regel oder Regelgruppe enthalten	Der Kontrolltitel wurde von A WAF Regional Web ACL sollte mindestens eine Regel oder Regelgruppe enthalten in AWS WAF Classic Regional Web ACLs sollte mindestens eine Regel oder Regelgruppe haben geändert.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
14. September 2023	[WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben	Der Titel des Steuerelements wurde von „Eine globale WAF-Regel sollte mindestens eine Bedingung haben“ zu „AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben“ geändert.
14. September 2023	[WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben	Der Titel des Steuerelements wurde von „Eine globale WAF-Regelgruppe sollte mindestens eine Regel haben“ zu „AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben“ geändert.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
14. September 2023	[WAF.8] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben	Der Steuerelementtitel wurde von Eine globale WAF-Web-ACL sollte mindestens eine Regel oder Regelgruppe haben zu AWS WAF Classic Global Web ACLs sollte mindestens eine Regel oder Regelgruppe haben geändert.
14. September 2023	[WAF.10] AWS WAF web ACLs sollte mindestens eine Regel oder Regelgruppe haben	Der Titel des Steuerelements wurde von Eine WAFv2 Web-ACL sollte mindestens eine Regel oder Regelgruppe haben zu AWS WAF Web ACLs sollte mindestens eine Regel oder Regelgruppe haben geändert.
14. September 2023	[WAF.11] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein	Der Titel des Steuerelements AWS WAF wurde von Version 2 geändert, die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
20. Juli 2023	[S3.4] Für S3-Buckets sollte die serverseitige Verschlüsselung aktiviert sein.	S3.4 prüft, ob für einen Amazon S3 S3-Bucket entweder die serverseitige Verschlüsselung aktiviert ist oder ob die S3-Bucket-Richtlinie PutObject Anfragen ohne serverseitige Verschlüsselung explizit ablehnt. Security Hub CSPM hat diese Steuerung aktualisiert und umfasst nun eine serverseitige Dual-Layer-Verschlüsselung mit KMS-Schlüsseln (DSSE-KMS). Das Steuerelement erzeugt einen erfolgreichen Befund, wenn ein S3-Bucket mit SSE-S3, SSE-KMS oder DSSE-KMS verschlüsselt ist.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
17. Juli 2023	[S3.17] S3-Allzweck-Buckets sollten im Ruhezustand verschlüsselt werden mit AWS KMS keys	S3.17 prüft, ob ein Amazon S3 S3-Bucket mit einem verschlüsselt ist. AWS KMS key Security Hub CSPM hat diese Steuerung aktualisiert und umfasst nun eine serverseitige Dual-Layer-Verschlüsselung mit KMS-Schlüsseln (DSSE-KMS). Wenn ein S3-Bucket mit SSE-KMS oder DSSE-KMS verschlüsselt ist, führt das Steuerelement zu einem erfolgreichen Ergebnis.
9. Juni 2023	[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	EKS.2 prüft, ob ein Amazon EKS-Cluster auf einer unterstützten Kubernetes-Version läuft. Die älteste unterstützte Version ist jetzt. 1.23

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
9. Juni 2023	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub CSPM unterstützt jetzt <code>ruby3.2</code> als Parameter.
5. Juni 2023	[APIGateway.5] API Gateway REST API-Cache-Daten sollten im Ruhezustand verschlüsselt werden	APIGateway.5 prüft, ob alle Methoden in den REST-API-Stufen von Amazon API Gateway im Ruhezustand verschlüsselt sind. Security Hub CSPM hat das Steuerelement aktualisiert, sodass die Verschlüsselung einer bestimmten Methode nur ausgewertet wird, wenn das Caching für diese Methode aktiviert ist.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
18. Mai 2023	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub CSPM unterstützt jetzt <code>java17</code> als Parameter.
18. Mai 2023	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub CSPM unterstützt nicht mehr <code>nodejs12.x</code> als Parameter.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
23. April 2023	[ECS.10] Die ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen	ECS.10 prüft, ob die Amazon ECS Fargate-Dienste die neueste Version der Fargate-Plattform ausführen. Kunden können Amazon ECS direkt über ECS oder mithilfe von ECS bereitgestellten CodeDeploy. Security Hub CSPM hat dieses Steuerelement aktualisiert, sodass es bei der Bereitstellung von ECS CodeDeploy Fargate-Diensten die Ergebnisse bestanden hat.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
20. April 2023	[S3.6] Allgemeine S3-Bucket-Richtlinien sollten den Zugriff auf andere einschränken AWS-Konten	S3.6 prüft, ob eine Bucket-Richtlinie von Amazon Simple Storage Service (Amazon S3) verhindert, dass Prinzipale AWS-Konten anderer Benutzer verweigerter Aktionen für Ressourcen im S3-Bucket ausführen. Security Hub CSPM hat die Steuerung aktualisiert, um Bedingungen in einer Bucket-Richtlinie zu berücksichtigen.
18. April 2023	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub CSPM unterstützt jetzt <code>python3.10</code> als Parameter.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
18. April 2023	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub CSPM unterstützt nicht mehr dotnetcore3.1 als Parameter.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
17. April 2023	[RDS.11] Bei RDS-Instances sollten automatische Backups aktiviert sein	RDS.11 prüft, ob für Amazon RDS-Instances automatische Backups aktiviert sind, wobei die Aufbewahrungsdauer für Backups mindestens sieben Tage beträgt. Security Hub CSPM hat diese Kontrolle aktualisiert, um Read Replicas von der Evaluierung auszuschließen, da nicht alle Engines automatische Backups auf Read Replicas unterstützen. Darüber hinaus bietet RDS nicht die Möglichkeit, bei der Erstellung von Read Replicas einen Aufbewahrungszeitraum für Backups anzugeben. Read Replicas werden standardmäßig mit einer Aufbewahrungsdauer für Backups erstellt. 0

Security Hub-Steuerungen für AWS-Konten

Diese Security Hub-Steuerelemente AWS-Konten werden ausgewertet.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[Account.1] Sicherheitskontaktinformationen sollten bereitgestellt werden für AWS-Konto

Verwandte Anforderungen: NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2)

Kategorie: Identifizieren > Ressourcenkonfiguration

Schweregrad: Mittel

Art der Ressource: AWS:::Account

AWS Config -Regel: [security-account-information-provided](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon Web Services (AWS) -Konto Sicherheitskontaktinformationen enthält. Die Kontrolle schlägt fehl, wenn keine Sicherheitskontaktinformationen für das Konto bereitgestellt werden.

Alternative Sicherheitskontakte AWS ermöglichen es, eine andere Person bei Problemen mit Ihrem Konto zu kontaktieren, falls Sie nicht verfügbar sind. Benachrichtigungen können von Support oder anderen AWS-Service Teams zu sicherheitsrelevanten Themen im Zusammenhang mit Ihrer AWS-Konto Nutzung stammen.

Abhilfe

Informationen zum Hinzufügen eines alternativen Kontakts als Sicherheitskontakt zu Ihrem AWS-Konto Ansprechpartner finden Sie unter [Aktualisieren der alternativen Kontakte für Sie AWS-Konto](#) im Referenzhandbuch zur AWS Kontoverwaltung.

[Account.2] AWS-Konten sollte Teil einer Organisation sein AWS Organizations

Kategorie: Schützen > Sicheres Zugriffsmanagement > Zugriffskontrolle

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2

Schweregrad: Hoch

Art der Ressource: AWS:::Account

AWS Config -Regel: [account-part-of-organizations](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob ein Teil einer Organisation AWS-Konto ist, die über verwaltet wird AWS Organizations. Die Kontrolle schlägt fehl, wenn das Konto nicht Teil einer Organisation ist.

Organizations hilft Ihnen dabei, Ihre Umgebung zentral zu verwalten, während Sie Ihre Workloads skalieren. AWS Sie können mehrere verwenden AWS-Konten , um Workloads zu isolieren, für die bestimmte Sicherheitsanforderungen gelten, oder um Frameworks wie HIPAA oder PCI einzuhalten. Durch die Gründung einer Organisation können Sie mehrere Konten als eine einzige Einheit verwalten und deren Zugriff AWS-Services, Ressourcen und Regionen zentral verwalten.

Abhilfe

Informationen zum Erstellen einer neuen Organisation und AWS-Konten zum automatischen Hinzufügen finden Sie unter [Organisation erstellen](#) im AWS Organizations Benutzerhandbuch. Informationen zum Hinzufügen von Konten zu einer bestehenden Organisation finden Sie im AWS Organizations Benutzerhandbuch unter [Einladen einer AWS-Konto Person, Ihrer Organisation beizutreten](#).

Security Hub-Steuerungen für AWS Amplify

Diese Security Hub-Steuerelemente bewerten den AWS Amplify Service und die Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[Amplify.1] Amplify-Apps sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Amplify::App`

AWS Config -Regel: [amplify-app-tagged](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Eine Liste der Tag-Schlüssel vom Typ „“, die einer ausgewerteten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS Amplify App über die im `requiredKeyTags` Parameter angegebenen Tag-Schlüssel verfügt. Das Steuerelement schlägt fehl, wenn die App keine Tag-Schlüssel oder nicht alle im `requiredKeyTags` Parameter angegebenen Schlüssel hat. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die App keine Tagschlüssel hat. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws:` Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen](#)

mit [ABAC-Autorisierung](#) im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im [Tagging AWS Resources and Tag Editor User Guide](#).

 Note

Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS Amplify App finden Sie unter [Unterstützung für Ressourcen-Tagging](#) im AWS Amplify Hosting-Benutzerhandbuch.

[Amplify.2] Amplify-Zweige sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Amplify::Branch`

AWS Config -Regel: [amplify-branch-tagged](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Eine Liste der Tag-Schlüssel vom Typ „“, die einer ausgewerteten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert

zwischen Groß- und Kleinschreibung unterschieden.

Dieses Steuerelement prüft, ob ein AWS Amplify Zweig über die im `requiredKeyTags` Parameter angegebenen Tagschlüssel verfügt. Das Steuerelement schlägt fehl, wenn der Zweig keine Tagschlüssel oder nicht alle im `requiredKeyTags` Parameter angegebenen Schlüssel hat. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Zweig keine Tagschlüssel hat. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws :` Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im [Tagging AWS Resources and Tag](#) Editor User Guide.

Note

Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS Amplify Branch finden Sie unter [Resource Tagging Support](#) im AWS Amplify Hosting-Benutzerhandbuch.

Security Hub-Steuerungen für Amazon API Gateway

Diese AWS Security Hub Kontrollen bewerten den Service und die Ressourcen von Amazon API Gateway. Die Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[APIGateway.1] API Gateway REST und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

AWS::ApiGateway::StageRessourcentyp:, AWS::ApiGatewayV2::Stage

AWS Config -Regel: [api-gw-execution-logging-enabled](#)

Art des Zeitplans: Änderung ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub
loggingLevel	Protokollierungsstufe	Enum	ERROR, INFO	No default value

Dieses Steuerelement prüft, ob in allen Phasen einer Amazon API Gateway Gateway-REST- oder WebSocket API-Phase die Protokollierung aktiviert ist. Die Kontrolle schlägt fehl, wenn loggingLevel nicht ERROR oder INFO für alle Stufen der API. Sofern Sie keine benutzerdefinierten Parameterwerte angeben, um anzugeben, dass ein bestimmter Protokolltyp aktiviert werden soll, erzeugt Security Hub eine erfolgreiche Feststellung, wenn die Protokollierungsebene entweder ERROR oder istINFO.

Für API Gateway REST- oder WebSocket API-Stufen sollten die entsprechenden Protokolle aktiviert sein. Die REST- und WebSocket API-Ausführungsprotokollierung von API Gateway bietet detaillierte Aufzeichnungen der Anfragen, die an die REST- und API-Stufen von WebSocket API Gateway gestellt wurden. Die Phasen umfassen Backend-Antworten zur API-Integration, Antworten des Lambda-Autorisierers und die requestId For-Integrationsendpunkte. AWS

Abhilfe

Informationen zum Aktivieren der Protokollierung für REST- und WebSocket API-Operationen finden Sie unter [CloudWatch API-Protokollierung mithilfe der API-Gateway-Konsole einrichten](#) im API Gateway Developer Guide.

[APIGateway.2] API Gateway REST API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden

Verwandte Anforderungen: NIST.800-53.r5 AC-1 7 (2), (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 NIST.800-53.r5 IA-5 (3), 3, 3, 3 (NIST.800-53.r5 SC-13), NIST.800-53.r5 SC-2 (4), NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-7 (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.R5 SI-7 NIST.800-53.r5 SC-8 (6), NIST.800-171.r2 3.13.15

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: AWS::ApiGateway::Stage

AWS Config -Regel: [api-gw-ssl-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für die REST-API-Stufen von Amazon API Gateway SSL-Zertifikate konfiguriert sind. Backend-Systeme verwenden diese Zertifikate, um zu authentifizieren, dass eingehende Anfragen von API Gateway stammen.

API Gateway-REST-API-Stufen sollten mit SSL-Zertifikaten konfiguriert werden, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Abhilfe

Detaillierte Anweisungen zum Generieren und Konfigurieren von API Gateway REST API-SSL-Zertifikaten finden Sie unter [Generieren und Konfigurieren eines SSL-Zertifikats für die Backend-Authentifizierung](#) im API Gateway Developer Guide.

[APIGateway.3] Bei den REST-API-Stufen von API Gateway sollte die AWS X-Ray Ablaufverfolgung aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-7

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Art der Ressource: AWS::ApiGateway::Stage

AWS Config -Regel: [api-gw-xray-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob AWS X-Ray Active Tracing für Ihre Amazon API Gateway Gateway-REST-API-Stufen aktiviert ist.

X-Ray Tracing ermöglicht eine schnellere Reaktion auf Leistungsänderungen der zugrunde liegenden Infrastruktur. Leistungsänderungen könnten zu einer mangelnden Verfügbarkeit der API führen. X-Ray Active Tracing bietet Echtzeit-Metriken zu Benutzeranfragen, die über Ihre API-Gateway-REST-API-Operationen und verbundenen Dienste fließen.

Abhilfe

Ausführliche Anweisungen zur Aktivierung von X-Ray Active Tracing für API Gateway REST-API-Operationen finden Sie unter [Amazon API Gateway Active Tracing Support for AWS X-Ray](#) im AWS X-Ray Developer Guide.

[APIGateway.4] API Gateway sollte mit einer WAF-Web-ACL verknüpft sein

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (21)

Kategorie: Schützen > Schutzdienste

Schweregrad: Mittel

Art der Ressource: AWS::ApiGateway::Stage

AWS Config -Regel: [api-gw-associated-with-waf](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine API Gateway Gateway-Stufe (ACL-Stufe) verwendet. AWS WAF Dieses Steuerelement schlägt fehl, wenn keine AWS WAF Web-ACL an eine REST-API-Gateway-Stufe angehängt ist.

AWS WAF ist eine webbasierte Firewall, die Webanwendungen schützt und Webanwendungen vor Angriffen APIs schützt. Sie ermöglicht ihnen, eine ACL-Regel zum Zulassen, Blockieren oder Zählen von Webanforderungen basierend auf von Ihnen definierten anpassbaren Web-Sicherheitsregeln und Bedingungen zu konfigurieren. Stellen Sie sicher, dass Ihre API Gateway Gateway-Stufe mit einer AWS WAF Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Abhilfe

Informationen zur Verknüpfung einer AWS WAF regionalen -Web-ACL mit einer bestehenden API-Gateway-API-Stufe finden Sie unter Using [AWS WAF to protect your APIs](#) im API Gateway Gateway-Entwicklerhandbuch.

[APIGateway.5] API Gateway REST API-Cache-Daten sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Schweregrad: Mittel

Art der Ressource: AWS::ApiGateway::Stage

AWS Config Regel: api-gw-cache-encrypted (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob alle Methoden in API Gateway REST API-Stufen, für die der Cache aktiviert ist, verschlüsselt sind. Die Steuerung schlägt fehl, wenn eine Methode in einer API Gateway Gateway-REST-API-Stufe für den Cache konfiguriert ist und der Cache nicht verschlüsselt ist. Security Hub bewertet die Verschlüsselung einer bestimmten Methode nur, wenn das Caching für diese Methode aktiviert ist.

Durch die Verschlüsselung von Daten im Ruhezustand wird das Risiko verringert, dass auf Daten, die auf der Festplatte gespeichert sind, von einem Benutzer zugegriffen wird, für den kein Benutzer authentifiziert ist. AWS Es fügt weitere Zugriffskontrollen hinzu, um den Zugriff unberechtigter Benutzer auf die Daten einzuschränken. Beispielsweise sind API-Berechtigungen erforderlich, um die Daten zu entschlüsseln, bevor sie gelesen werden können.

API-Gateway-REST-API-Caches sollten im Ruhezustand verschlüsselt werden, um eine zusätzliche Sicherheitsebene zu gewährleisten.

Abhilfe

Informationen zur Konfiguration von API-Caching für eine Phase finden Sie unter [Amazon API Gateway Gateway-Caching aktivieren](#) im API Gateway Developer Guide. Wählen Sie in den Cache-Einstellungen die Option Cache-Daten verschlüsseln.

[APIGateway.8] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben

Verwandte Anforderungen: NIST.800-53.r5 AC-3, NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2)

Kategorie: Schützen > Sicheres Zugriffsmanagement

Schweregrad: Mittel

Art der Ressource: AWS::ApiGatewayV2::Route

AWS Config -Regel: [api-gwv2-authorization-type-configured](#)

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub
authorizationType	Autorisierungstyp der API-Routen	Enum	AWS_IAM, CUSTOM, JWT	Kein Standardwert

Diese Kontrolle prüft, ob für die Amazon API Gateway Gateway-Routen einen Autorisierungstyp haben. Die Steuerung schlägt fehl, wenn die API-Gateway-Route keinen Autorisierungstyp hat. Optional können Sie einen benutzerdefinierten Parameterwert angeben, wenn das Steuerelement nur dann übergeben werden soll, wenn die Route den im authorizationType Parameter angegebenen Autorisierungstyp verwendet.

API Gateway unterstützt mehrere Mechanismen zur Steuerung und Verwaltung des Zugriffs auf Ihre API. Durch die Angabe eines Autorisierungstyps können Sie den Zugriff auf Ihre API auf autorisierte Benutzer oder Prozesse beschränken.

Abhilfe

Informationen zum Festlegen eines Autorisierungstyps für HTTP APIs finden Sie unter [Steuern und Verwalten des Zugriffs auf eine HTTP-API im API Gateway](#) im API Gateway Gateway-Entwicklerhandbuch. Informationen zum Festlegen eines WebSocket APIs Autorisierungstyps für finden Sie unter [Steuern und Verwalten des Zugriffs auf eine WebSocket API im API Gateway](#) im API Gateway.

[APIGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (26), (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-7 NIST.800-53.r5 SC-7 (8), PCI DSS v4.0.1/10.4.2

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS::ApiGatewayV2::Stage

AWS Config -Regel: [api-gwv2-access-logs-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob für die V2-Stufen von Amazon API Gateway die Zugriffsprotokollierung konfiguriert ist. Diese Kontrolle schlägt fehl, wenn die Einstellungen für das Zugriffsprotokoll nicht definiert sind.

API Gateway Gateway-Zugriffsprotokolle enthalten detaillierte Informationen darüber, wer auf Ihre API zugegriffen hat und wie der Aufrufer auf die API zugegriffen hat. Diese Protokolle sind für Anwendungen wie Sicherheits- und Zugriffsprüfungen sowie forensische Untersuchungen nützlich. Aktivieren Sie diese Zugriffsprotokolle, um Verkehrsmuster zu analysieren und Probleme zu beheben.

Weitere bewährte Methoden finden Sie unter [Monitoring REST APIs](#) im API Gateway Developer Guide.

Abhilfe

Informationen zum Einrichten der Zugriffsprotokollierung finden Sie unter [CloudWatch API-Protokollierung mithilfe der API-Gateway-Konsole einrichten](#) im API Gateway Developer Guide.

Security Hub-Steuerungen für AWS AppConfig

Diese Security Hub-Steuerelemente bewerten den AWS AppConfig Service und die Ressourcen.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[AppConfig.1] AWS AppConfig Anwendungen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::AppConfig::Application

AWS Config -Regel: appconfig-application-tagged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS AppConfig Anwendung über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredKeyTags` definiert sind. Das Steuerelement schlägt fehl, wenn die Anwendung keine Tagschlüssel hat oder wenn nicht alle im Parameter angegebenen Schlüssel vorhanden sind `requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Anwendung mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS AppConfig Anwendung finden Sie unter [TagResource](#) in der API-Referenz zu AWS AppConfig

[AppConfig.2] AWS AppConfig Konfigurationsprofile sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::AppConfig::ConfigurationProfile`

AWS Config -Regel: `appconfig-configuration-profile-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS AppConfig Konfigurationsprofil Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredKeyTags` definiert sind. Das Steuerelement schlägt fehl, wenn das Konfigurationsprofil keine Tagschlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel enthält `requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Konfigurationsprofil mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` , werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS AppConfig Konfigurationsprofil finden Sie unter [TagResource](#) in der API-Referenz zu AWS AppConfig

[AppConfig.3] AWS AppConfig Umgebungen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::AppConfig::Environment`

AWS Config -Regel: `appconfig-environment-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS AppConfig Umgebung über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredKeyTags` definiert sind. Das Steuerelement schlägt fehl, wenn die Umgebung keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat `requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Umgebung mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen

anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS AppConfig Umgebung finden Sie unter [TagResource](#) in der API-Referenz zu AWS AppConfig

[AppConfig.4] AWS AppConfig Erweiterungszuordnungen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::AppConfig::ExtensionAssociation`

AWS Config -Regel: `appconfig-extension-association-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS	Kein Standardwert

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen.	

Dieses Steuerelement prüft, ob eine AWS AppConfig Erweiterungsassoziation Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredKeyTags` definiert sind. Das Steuerelement schlägt fehl, wenn die Erweiterungszuordnung keine Tagschlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält `requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Erweiterungsverknüpfung mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` , werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter

AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS AppConfig Erweiterungsverknüpfung finden Sie unter [TagResource](#) in der API-Referenz zu AWS AppConfig

Security Hub-Steuerelemente für Amazon AppFlow

Diese Security Hub Hub-Kontrollen bewerten den AppFlow Service und die Ressourcen von Amazon.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[AppFlow.1] AppFlow Amazon-Datenflüsse sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::AppFlow::Flow

AWS Config -Regel: appflow-flow-tagged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
requiredKeyTags	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß-	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert

und Kleinschreibung unterscheiden.

Dieses Steuerelement prüft, ob ein AppFlow Amazon-Flow Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind `requiredKeyTags`. Die Steuerung schlägt fehl, wenn der Flow keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält `requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Flow mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `aws:` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AppFlow Amazon-Flow finden Sie unter [Erstellen von Flows AppFlow in Amazon](#) im AppFlow Amazon-Benutzerhandbuch.

Security Hub-Steuerungen für AWS App Runner

Diese AWS Security Hub Kontrollen bewerten den AWS App Runner Service und die Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[AppRunner.1] App Runner-Dienste sollten markiert sein

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::AppRunner::Service`

AWS Config -Regel: [apprunner-service-tagged](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS App Runner Service über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredKeyTags` definiert sind. Das Steuerelement schlägt fehl, wenn der App Runner-Dienst keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter

angegebenen Schlüssel `requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der App Runner-Dienst mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS App Runner Service finden Sie unter [TagResource](#) in der API-Referenz zu AWS App Runner

[AppRunner.2] App Runner VPC-Konnektoren sollten markiert sein

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::AppRunner::VpcConnector`

AWS Config -Regel: [apprunner-vpc-connector-tagged](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS App Runner VPC-Connector Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredKeyTags` definiert sind. Die Steuerung schlägt fehl, wenn der VPC-Connector keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter `requiredKeyTags` angegebenen Schlüssel hat. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der VPC-Connector mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere

Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS App Runner VPC-Connector finden Sie unter [TagResource](#) in der API-Referenz zu AWS App Runner

Security Hub-Steuerungen für AWS AppSync

Diese Security Hub-Steuerelemente bewerten den AWS AppSync Service und die Ressourcen.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[AppSync.1] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: `AWS::AppSync::GraphQLApi`

AWS Config -Regel: [appsync-cache-ct-encryption-at-rest](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein AWS AppSync API-Cache im Ruhezustand verschlüsselt ist. Die Steuerung schlägt fehl, wenn der API-Cache im Ruhezustand nicht verschlüsselt ist.

Daten im Ruhezustand beziehen sich auf Daten, die für einen beliebigen Zeitraum in einem persistenten, nichtflüchtigen Speicher gespeichert werden. Durch die Verschlüsselung ruhender

Daten können Sie deren Vertraulichkeit schützen, wodurch das Risiko verringert wird, dass ein nicht autorisierter Benutzer darauf zugreifen kann.

Abhilfe

Sie können die Verschlüsselungseinstellungen nicht mehr ändern, nachdem Sie das Caching für Ihre AWS AppSync API aktiviert haben. Stattdessen müssen Sie den Cache löschen und ihn mit aktivierter Verschlüsselung neu erstellen. Weitere Informationen finden Sie unter [Cache-Verschlüsselung](#) im AWS AppSync Entwicklerhandbuch.

[AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben

Verwandte Anforderungen: PCI DSS v4.0.1/10.4.2

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS::AppSync::GraphQLApi

AWS Config -Regel: [appsync-logging-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert	
fieldLoggingLevel	Ebene der Feldprotokollierung	Enum	ERROR, ALL, INFO, DEBUG	No default value	

Dieses Steuerelement prüft, ob für eine AWS AppSync API die Protokollierung auf Feldebene aktiviert ist. Das Steuerelement schlägt fehl, wenn die Protokollebene des Field Resolvers auf Keine gesetzt ist. Sofern Sie keine benutzerdefinierten Parameterwerte angeben, um anzugeben, dass ein bestimmter Protokolltyp aktiviert werden soll, erzeugt Security Hub eine erfolgreiche Suche, wenn die Protokollebene des Feldauflösers entweder ERROR oder ALL ist.

Sie können die Protokollierung und Metriken verwenden, um Ihre GraphQL-Abfragen zu identifizieren, Fehler darin zu beheben und sie zu optimieren. Wenn Sie die Protokollierung für AWS AppSync GraphQL aktivieren, erhalten Sie detaillierte Informationen zu API-Anfragen und -Antworten, können Probleme identifizieren und darauf reagieren und gesetzliche Anforderungen erfüllen.

Abhilfe

Informationen zum Aktivieren der Protokollierung für AWS AppSync finden Sie unter [Einrichtung und Konfiguration](#) im AWS AppSync Entwicklerhandbuch.

[AppSync.4] AWS AppSync GraphQL APIs sollte markiert sein

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::AppSync::GraphQLApi`

AWS Config Regel: `tagged-appsync-graphqlapi` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS AppSync GraphQL-API Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn die GraphQL-API keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter

`requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die GraphQL-API mit keinem Schlüssel gekennzeichnet ist. System-Tags, die automatisch angewendet werden und mit `beginnenaws :` , werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS AppSync GraphQL-API finden Sie unter [TagResource](#) in der API-Referenz zu AWS AppSync

[AppSync.5] AWS AppSync GraphQL APIs sollte nicht mit API-Schlüsseln authentifiziert werden

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15) NIST.800-53.r5 AC-3, (7), NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6

Kategorie: Schützen > Sichere Zugriffsverwaltung > Passwortlose Authentifizierung

Schweregrad: Hoch

Art der Ressource: `AWS::AppSync::GraphQLApi`

AWS Config -Regel: [appsync-authorization-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `AllowedAuthorizationTypes`: `AWS_LAMBDA`, `AWS_IAM`, `OPENID_CONNECT`, `AMAZON_COGNITO_USER_POOLS` (nicht anpassbar)

Dieses Steuerelement prüft, ob Ihre Anwendung einen API-Schlüssel verwendet, um mit einer AWS AppSync GraphQL-API zu interagieren. Die Steuerung schlägt fehl, wenn eine AWS AppSync GraphQL-API mit einem API-Schlüssel authentifiziert wird.

Ein API-Schlüssel ist ein fest codierter Wert in Ihrer Anwendung, der vom AWS AppSync Dienst generiert wird, wenn Sie einen nicht authentifizierten GraphQL-Endpunkt erstellen. Wenn dieser API-Schlüssel kompromittiert ist, ist Ihr Endpunkt anfällig für unbeabsichtigten Zugriff. Sofern Sie keine öffentlich zugängliche Anwendung oder Website unterstützen, empfehlen wir nicht, einen API-Schlüssel für die Authentifizierung zu verwenden.

Abhilfe

Informationen zum Einrichten einer Autorisierungsoption für Ihre AWS AppSync GraphQL-API finden Sie unter [Autorisierung und Authentifizierung](#) im AWS AppSync Entwicklerhandbuch.

[AppSync.6] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: `AWS::AppSync::ApiCache`

AWS Config -Regel: [appsync-cache-ct-encryption-in-transit](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein AWS AppSync API-Cache während der Übertragung verschlüsselt ist. Die Steuerung schlägt fehl, wenn der API-Cache bei der Übertragung nicht verschlüsselt wird.

Daten während der Übertragung beziehen sich auf Daten, die von einem Ort an einen anderen übertragen werden, z. B. zwischen Knoten in Ihrem Cluster oder zwischen Ihrem Cluster und Ihrer Anwendung. Daten können über das Internet oder innerhalb eines privaten Netzwerks übertragen werden. Durch die Verschlüsselung von Daten während der Übertragung wird das Risiko verringert, dass ein nicht autorisierter Benutzer den Netzwerkverkehr abhören kann.

Abhilfe

Sie können die Verschlüsselungseinstellungen nicht mehr ändern, nachdem Sie das Caching für Ihre API aktiviert haben. AWS AppSync Stattdessen müssen Sie den Cache löschen und ihn mit aktivierter Verschlüsselung neu erstellen. Weitere Informationen finden Sie unter [Cache-Verschlüsselung](#) im AWS AppSync Entwicklerhandbuch.

Security Hub-Steuerelemente für Amazon Athena

Diese AWS Security Hub Kontrollen bewerten den Service und die Ressourcen von Amazon Athena. Die Steuerelemente sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[Athena.1] Athena-Arbeitsgruppen sollten im Ruhezustand verschlüsselt werden

Important

Security Hub hat diese Kontrolle im April 2024 eingestellt. Weitere Informationen finden Sie unter [Änderungsprotokoll für Security Hub CSPM-Steuerelemente](#).

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Schweregrad: Mittel

Art der Ressource: AWS::Athena::WorkGroup

AWS Config -Regel: [athena-workgroup-encrypted-at-rest](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Athena-Arbeitsgruppe im Ruhezustand verschlüsselt ist. Die Steuerung schlägt fehl, wenn eine Athena-Arbeitsgruppe im Ruhezustand nicht verschlüsselt ist.

In Athena können Sie Arbeitsgruppen erstellen, um Abfragen für Teams, Anwendungen oder verschiedene Workloads auszuführen. Jede Arbeitsgruppe hat eine Einstellung, um die Verschlüsselung für alle Abfragen zu aktivieren. Sie haben die Möglichkeit, serverseitige Verschlüsselung mit von Amazon Simple Storage Service (Amazon S3) verwalteten Schlüsseln, serverseitige Verschlüsselung mit AWS Key Management Service (AWS KMS) -Schlüsseln oder clientseitige Verschlüsselung mit kundenverwalteten KMS-Schlüsseln zu verwenden. Daten im Ruhezustand beziehen sich auf alle Daten, die für einen beliebigen Zeitraum in einem persistenten, nichtflüchtigen Speicher gespeichert werden. Durch Verschlüsselung können Sie die Vertraulichkeit solcher Daten schützen und so das Risiko verringern, dass ein unberechtigter Benutzer darauf zugreifen kann.

Abhilfe

Informationen zum Aktivieren der Verschlüsselung im Ruhezustand für Athena-Arbeitsgruppen finden Sie unter [Bearbeiten einer Arbeitsgruppe](#) im Amazon Athena Athena-Benutzerhandbuch. Wählen Sie im Abschnitt Konfiguration der Abfrageergebnisse die Option Abfrageergebnisse verschlüsseln aus.

[Athena.2] Athena-Datenkataloge sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::Athena::DataCatalog

AWS Config Regel: tagged-athena-datacatalog (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob ein Amazon Athena Athena-Datenkatalog Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn der Datenkatalog keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Datenkatalog mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Athena-Datenkatalog finden Sie unter [Tagging Athena-Ressourcen im Amazon Athena](#) Athena-Benutzerhandbuch.

[Athena.3] Athena-Arbeitsgruppen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::Athena::WorkGroup

AWS Config Regel: tagged-athena-workgroup (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
requiredTagKeys	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob eine Amazon Athena Athena-Arbeitsgruppe Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind. `requiredTagKeys` Die Steuerung schlägt fehl, wenn die Arbeitsgruppe keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat. `requiredTagKeys` Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Arbeitsgruppe mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` , werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Stichwörtern zu einer Athena-Arbeitsgruppe finden Sie unter [Hinzufügen und Löschen von Stichwörtern in einer einzelnen Arbeitsgruppe](#) im Amazon Athena Athena-Benutzerhandbuch.

[Athena.4] Bei Athena-Arbeitsgruppen sollte die Protokollierung aktiviert sein

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS::Athena::WorkGroup

AWS Config -Regel: [athena-workgroup-logging-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für eine Amazon Athena Athena-Arbeitsgruppe die Protokollierung aktiviert ist. Die Steuerung schlägt fehl, wenn für die Arbeitsgruppe die Protokollierung nicht aktiviert ist.

In Auditprotokollen werden Systemaktivitäten verfolgt und überwacht. Sie bieten eine Aufzeichnung von Ereignissen, anhand derer Sie Sicherheitsverletzungen erkennen, Vorfälle untersuchen und Vorschriften einhalten können. Auditprotokolle verbessern auch die allgemeine Rechenschaftspflicht und Transparenz Ihres Unternehmens.

Abhilfe

Informationen zur Aktivierung der Protokollierung für eine Athena-Arbeitsgruppe finden Sie unter [Aktivieren von CloudWatch Abfragemetriken in Athena im Amazon Athena Benutzerhandbuch](#).

Security Hub-Steuerungen für AWS Backup

Diese Security Hub-Steuerelemente bewerten den AWS Backup Service und die Ressourcen.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein

Verwandte Anforderungen: NIST.800-53.R5 CP-9 (8), NIST.800-53.R5 SI-12

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: AWS::Backup::RecoveryPoint

AWS Config -Regel: [backup-recovery-point-encrypted](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein AWS Backup Wiederherstellungspunkt im Ruhezustand verschlüsselt ist. Die Steuerung schlägt fehl, wenn der Erholungspunkt im Ruhezustand nicht verschlüsselt ist.

Ein AWS Backup Wiederherstellungspunkt bezieht sich auf eine bestimmte Kopie oder einen Snapshot von Daten, der im Rahmen eines Backup-Vorgangs erstellt wird. Er stellt einen bestimmten Zeitpunkt dar, zu dem die Daten gesichert wurden, und dient als Wiederherstellungspunkt für den Fall, dass die Originaldaten verloren gehen, beschädigt werden oder nicht mehr zugänglich sind. Die Verschlüsselung der Backup-Wiederherstellungspunkte bietet zusätzlichen Schutz vor unbefugtem Zugriff. Die Verschlüsselung ist eine bewährte Methode zum Schutz der Vertraulichkeit, Integrität und Sicherheit von Backup-Daten.

Abhilfe

Informationen zur Verschlüsselung eines AWS Backup Wiederherstellungspunkts finden Sie unter [Verschlüsselung für Backups AWS Backup im AWS Backup](#) Entwicklerhandbuch.

[Backup.2] AWS Backup Wiederherstellungspunkte sollten markiert werden

Kategorie: Identifizieren > Inventar > Kennzeichnung

Schweregrad: Niedrig

Art der Ressource: AWS::Backup::RecoveryPoint

AWS Config Regel: tagged-backup-recoverypoint (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS Backup Wiederherstellungspunkt über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn der Erholungspunkt keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Erholungspunkt mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

So fügen Sie einem AWS Backup Recovery Point Tags hinzu

1. Öffnen Sie die AWS Backup Konsole unter <https://console.aws.amazon.com/backup>.
2. Wählen Sie im Navigationsbereich Backup-Pläne aus.
3. Wählen Sie einen Backup-Plan aus der Liste aus.
4. Wählen Sie im Abschnitt Backup-Plan-Tags die Option Tags verwalten aus.
5. Geben Sie den Schlüssel und den Wert für den Tags (Markierungen) ein. Wählen Sie Neues Tag hinzufügen für weitere Schlüssel-Wert-Paare.
6. Wenn Sie mit dem Hinzufügen der Tags fertig sind, wählen Sie Speichern.

[Backup.3] AWS Backup Tresore sollten markiert sein

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::Backup::BackupVault

AWS Config Regel: tagged-backup-backupvault (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS Backup Tresor über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn der Recovery Point keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Erholungspunkt mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

So fügen Sie Tags zu einem Tresor hinzu AWS Backup

1. Öffnen Sie die AWS Backup Konsole unter <https://console.aws.amazon.com/backup>.
2. Wählen Sie im Navigationsbereich Backup vaults (Sicherungstresore) aus.
3. Wählen Sie einen Backup-Tresor aus der Liste aus.
4. Wählen Sie im Abschnitt Backup-Tresor-Tags die Option Tags verwalten aus.
5. Geben Sie den Schlüssel und den Wert für den Tags (Markierungen) ein. Wählen Sie Neues Tag hinzufügen für weitere Schlüssel-Wert-Paare.
6. Wenn Sie mit dem Hinzufügen der Tags fertig sind, wählen Sie Speichern.

[Backup.4] AWS Backup Berichtspläne sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::Backup::ReportPlan

AWS Config Regel: tagged-backup-reportplan (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS Backup Berichtsplan Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn der Berichtsplan keine Tagschlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Berichtsplan mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Sie fügen Sie Stichwörter zu einem Berichtsplan AWS Backup hinzu

1. Öffnen Sie die AWS Backup Konsole unter <https://console.aws.amazon.com/backup>.
2. Wählen Sie im Navigationsbereich Backup vaults (Sicherungstresore) aus.
3. Wählen Sie einen Backup-Tresor aus der Liste aus.
4. Wählen Sie im Abschnitt Backup-Tresor-Tags die Option Tags verwalten aus.
5. Wählen Sie Neues Tag hinzufügen aus. Geben Sie den Schlüssel und den Wert für den Tags (Markierungen) ein. Wiederholen Sie den Vorgang für weitere Schlüssel-Wert-Paare.
6. Wenn Sie mit dem Hinzufügen der Tags fertig sind, wählen Sie Speichern.

[Backup.5] AWS Backup Backup-Pläne sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::Backup::BackupPlan

AWS Config Regel: tagged-backup-backupplan (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS Backup Backup-Plan Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn der Backup-Plan keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Backup-Plan mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

So fügen Sie Stichwörter zu einem Backup-Plan AWS Backup hinzu

1. Öffnen Sie die AWS Backup Konsole unter <https://console.aws.amazon.com/backup>.
2. Wählen Sie im Navigationsbereich Backup vaults (Sicherungstresore) aus.
3. Wählen Sie einen Backup-Tresor aus der Liste aus.
4. Wählen Sie im Abschnitt Backup-Tresor-Tags die Option Tags verwalten aus.
5. Wählen Sie Neues Tag hinzufügen aus. Geben Sie den Schlüssel und den Wert für den Tags (Markierungen) ein. Wiederholen Sie den Vorgang für weitere Schlüssel-Wert-Paare.
6. Wenn Sie mit dem Hinzufügen der Tags fertig sind, wählen Sie Speichern.

Security Hub-Steuerungen für AWS Batch

Diese Security Hub-Steuerelemente bewerten den AWS Batch Service und die Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[Batch.1] Warteschlangen für Batch-Jobs sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::Batch::JobQueue

AWS Config -Regel: [batch-job-queue-tagged](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS Batch Auftragswarteschlange Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredKeyTags` definiert sind. Das Steuerelement schlägt fehl, wenn die Auftragswarteschlange keine Tagschlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält `requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Auftragswarteschlange mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Stichwörtern zu einer Batch-Job-Warteschlange finden Sie unter [Taggen Ihrer Ressourcen](#) im AWS Batch Benutzerhandbuch.

[Batch.2] Richtlinien für die Batch-Planung sollten gekennzeichnet sein

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Batch::SchedulingPolicy`

AWS Config -Regel: [batch-scheduling-policy-tagged](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS Batch Planungsrichtlinie Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredKeyTags` definiert sind. Das Steuerelement schlägt fehl, wenn die Planungsrichtlinie keine Tagschlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält `requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Scheduling-Richtlinie mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Batch-Planungsrichtlinie finden Sie unter [Taggen Ihrer Ressourcen](#) im AWS Batch Benutzerhandbuch.

[Batch.3] Batch-Computing-Umgebungen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Batch::ComputeEnvironment`

AWS Config -Regel: [batch-compute-environment-tagged](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS Batch Rechenumgebung über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredKeyTags` definiert sind. Das Steuerelement schlägt fehl, wenn die Rechenumgebung keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat `requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Rechenumgebung mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` , werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen

anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Batch-Computing-Umgebung finden Sie unter [Taggen Ihrer Ressourcen](#) im AWS Batch Benutzerhandbuch.

[Batch.4] Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Batch::ComputeEnvironment`

AWS Config -Regel: [batch-managed-compute-env-compute-resources-tagged](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Eine Liste der Tag-Schlüssel vom Typ „“, die einer ausgewerteten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob die Eigenschaft `Compute Resources` in einer verwalteten AWS Batch Rechenumgebung über die durch den `requiredKeyTags` Parameter angegebenen Tag-Schlüssel verfügt. Das Steuerelement schlägt fehl, wenn die Eigenschaft „`Compute Resources`“ keine Tag-Schlüssel oder nicht alle durch den `requiredKeyTags` Parameter angegebenen Schlüssel enthält. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn eine `Compute-Resources`-Eigenschaft keine Tag-Schlüssel hat. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws:` Präfix haben. Dieses Steuerelement bewertet weder unverwaltete Computerumgebungen noch verwaltete Umgebungen, die Ressourcen verbrauchen AWS Fargate .

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im [Tagging AWS Resources and Tag Editor User Guide](#).

 Note

Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Tags zu Rechenressourcen in einer verwalteten AWS Batch Rechenumgebung finden Sie unter [Taggen Ihrer Ressourcen](#) im AWS Batch Benutzerhandbuch.

Security Hub Hub-Kontrollen für AWS Certificate Manager

Diese AWS Security Hub Kontrollen bewerten den AWS Certificate Manager (ACM) -Service und die Ressourcen. Die Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[ACM.1] Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden

Verwandte Anforderungen: NIST.800-53.r5 SC-2 8 (3), NIST.800-53.r5 SC-7 (16), NIST.800-171.R2 3.13.15, PCI DSS v4.0.1/4.2.1

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: AWS::ACM::Certificate

AWS Config -Regel: [acm-certificate-expiration-check](#)

Art des Zeitplans: Ausgelöste und periodische Änderung

Parameter:

Parameter	Beschreibung	Typ	Allowed values	Security Hub
daysToExpiration	Anzahl der Tage, innerhalb derer das ACM-Zertifikat erneuert werden muss	Ganzzahl	14 auf 365	30

Diese Kontrolle prüft, ob ein AWS Certificate Manager (ACM-) Zertifikat innerhalb des angegebenen Zeitraums erneuert wird. Es überprüft sowohl importierte Zertifikate als auch von ACM bereitgestellte Zertifikate. Die Kontrolle schlägt fehl, wenn das Zertifikat nicht innerhalb des angegebenen Zeitraums erneuert wird. Sofern Sie keinen benutzerdefinierten Parameterwert für den Verlängerungszeitraum angeben, verwendet Security Hub einen Standardwert von 30 Tagen.

ACM kann Zertifikate, die DNS-Validierung verwenden, automatisch verlängern. Bei Zertifikaten, die E-Mail-Validierung verwenden, müssen Sie auf eine E-Mail zur Domaininvalidierung antworten. ACM verlängert von Ihnen importierte Zertifikate nicht automatisch. Sie müssen importierte Zertifikate manuell erneuern.

Abhilfe

ACM bietet eine verwaltete Erneuerung für Ihre von Amazon ausgestellte SSL-/TLS-Zertifikate. Dies bedeutet, dass ACM Ihre Zertifikate entweder automatisch erneuert (wenn Sie die DNS-Validierung verwenden), oder es sendet Ihnen E-Mail-Benachrichtigungen, wenn der Ablauf des Zertifikats nähert. Diese Dienste werden sowohl für öffentliche als auch für private ACM-Zertifikate bereitgestellt.

Für Domänen, die per E-Mail validiert wurden

Wenn ein Zertifikat 45 Tage vor Ablauf abläuft, sendet ACM für jeden Domainnamen eine E-Mail an den Domaininhaber. Um die Domains zu validieren und die Verlängerung abzuschließen, müssen Sie auf die E-Mail-Benachrichtigungen antworten.

Weitere Informationen finden Sie im AWS Certificate Manager Benutzerhandbuch unter [Verlängerung für per E-Mail validierte Domains](#).

Für von DNS validierte Domänen

ACM erneuert automatisch Zertifikate, die DNS-Validierung verwenden. 60 Tage vor Ablauf überprüft ACM, ob das Zertifikat erneuert werden kann.

Wenn ein Domainname nicht validiert werden kann, sendet ACM eine Benachrichtigung, dass eine manuelle Validierung erforderlich ist. Diese Benachrichtigungen werden 45 Tage, 30 Tage, 7 Tage und 1 Tag vor Ablauf gesendet.

Weitere Informationen finden Sie im AWS Certificate Manager Benutzerhandbuch unter [Verlängerung für durch DNS validierte Domains](#).

[ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden

Verwandte Anforderungen: PCI DSS v4.0.1/4.2.1

Kategorie: Identifizieren > Inventar > Inventardienste

Schweregrad: Hoch

Art der Ressource: AWS::ACM::Certificate

AWS Config -Regel: [acm-certificate-rsa-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob RSA-Zertifikate, die mit verwaltet werden, eine Schlüssellänge von mindestens 2.048 Bit AWS Certificate Manager verwenden. Die Steuerung schlägt fehl, wenn die Schlüssellänge kleiner als 2.048 Bit ist.

Die Stärke der Verschlüsselung korreliert direkt mit der Schlüsselgröße. Wir empfehlen Schlüssellängen von mindestens 2.048 Bit, um Ihre AWS Ressourcen zu schützen, da Rechenleistung immer günstiger wird und Server immer fortschrittlicher werden.

Abhilfe

Die Mindestschlüssellänge für von ACM ausgestellte RSA-Zertifikate beträgt bereits 2.048 Bit. Anweisungen zur Ausstellung neuer RSA-Zertifikate mit ACM finden Sie unter Zertifikate [ausstellen und verwalten](#) im Benutzerhandbuch.AWS Certificate Manager

Mit ACM können Sie zwar Zertifikate mit kürzeren Schlüssellängen importieren, Sie müssen jedoch Schlüssel mit mindestens 2.048 Bit verwenden, um diese Kontrolle zu bestehen. Sie können die Schlüssellänge nach dem Importieren eines Zertifikats nicht ändern. Stattdessen müssen Sie Zertifikate mit einer Schlüssellänge von weniger als 2.048 Bit löschen. Weitere Informationen zum

Importieren von Zertifikaten in ACM finden Sie unter [Voraussetzungen für den Import von Zertifikaten](#) im AWS Certificate Manager -Leitfaden.

[ACM.3] ACM-Zertifikate sollten mit einem Tag versehen werden

Kategorie: Identifizieren > Inventar > Kennzeichnung

Schweregrad: Niedrig

Art der Ressource: `AWS::ACM::Certificate`

AWS Config Regel: `tagged-acm-certificate` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Allowed values	Security Hub
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS Certificate Manager (ACM-) Zertifikat Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind. `requiredTagKeys` Die Kontrolle schlägt fehl, wenn das Zertifikat keine Tagschlüssel hat oder wenn es nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Zertifikat mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` , werden ignoriert.

Ein Tag ist eine Markierung, die Sie einer AWS -Ressource zuordnen. Sie besteht aus einem Schlüssel und einem optionalen -Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Tags können Ihnen helfen, -Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Mithilfe von

Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC — Attribute-based access control) als Autorisierungsstrategie implementieren, die Berechtigungen auf der Grundlage von Tags definiert. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und AWS -Ressourcen anfügen. Sie können eine einzelne ABAC-Richtlinie oder einen separaten Richtlinienatz für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen zugelassen werden, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Was ist ABAC für AWS?](#) im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbare Informationen (PII) oder andere vertrauliche Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, einschließlich AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem ACM-Zertifikat finden Sie unter Kennzeichen [von AWS Certificate Manager Zertifikaten im Benutzerhandbuch](#).AWS Certificate Manager

Security Hub-Steuerungen für AWS CloudFormation

Diese Security Hub-Steuerelemente bewerten den AWS CloudFormation Service und die Ressourcen.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[CloudFormation.1] CloudFormation Stacks sollten in Simple Notification Service (SNS) integriert werden

 Important

Security Hub hat diese Kontrolle im April 2024 eingestellt. Weitere Informationen finden Sie unter [Änderungsprotokoll für Security Hub CSPM-Steuerelemente](#).

Verwandte Anforderungen: NIST.800-53.R5 SI-4 (12), NIST.800-53.R5 SI-4 (5)

Kategorie: Erkennen > Erkennungsdienste > Anwendungsüberwachung

Schweregrad: Niedrig

Art der Ressource: AWS::CloudFormation::Stack

AWS Config -Regel: [cloudformation-stack-notification-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob eine Amazon Simple Notification Service-Benachrichtigung in einen AWS CloudFormation Stack integriert ist. Die Kontrolle schlägt für einen CloudFormation Stack fehl, wenn ihm keine SNS-Benachrichtigung zugeordnet ist.

Wenn Sie eine SNS-Benachrichtigung mit Ihrem CloudFormation Stack konfigurieren, können Sie die Beteiligten sofort über alle Ereignisse oder Änderungen informieren, die im Stack auftreten.

Abhilfe

Informationen zur Integration eines CloudFormation Stacks und eines SNS-Themas finden Sie unter [Stacks direkt aktualisieren](#) im AWS CloudFormation Benutzerhandbuch.

[CloudFormation.2] CloudFormation Stapel sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::CloudFormation::Stack

AWS Config Regel: tagged-cloudformation-stack (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS CloudFormation Stack Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn der Stack keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Stack mit keinem Schlüssel gekennzeichnet ist. System-Tags, die automatisch angewendet werden und mit `beginnewaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem CloudFormation Stack finden Sie [CreateStack](#) in der AWS CloudFormation API-Referenz.

Security Hub-Steuerelemente für Amazon CloudFront

Diese AWS Security Hub Kontrollen bewerten den CloudFront Service und die Ressourcen von Amazon. Die Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein

Verwandte Anforderungen: NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), PCI DSS v4.0.1/2.2.6

Kategorie: Schützen > Sicheres Zugriffsmanagement > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Hoch

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config -Regel: [cloudfront-default-root-object-configured](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine CloudFront Amazon-Distribution so konfiguriert ist, dass sie ein bestimmtes Objekt zurückgibt, das das Standard-Root-Objekt ist. Die Steuerung schlägt fehl, wenn für die CloudFront Verteilung kein Standard-Stammobjekt konfiguriert ist.

Ein Benutzer kann manchmal die Stamm-URL der Distribution anstelle eines Objekts in der Distribution anfordern. In diesem Fall können Sie durch die Festlegung eines Standardstammobjekt verhindern, dass die Inhalte Ihrer Web-Verteilung preisgegeben werden.

Abhilfe

Informationen zur Konfiguration eines Standard-Root-Objekts für eine CloudFront Distribution finden Sie unter [How to specify a default root object](#) im Amazon CloudFront Developer Guide.

[CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen

Verwandte Anforderungen: NIST.800-53.r5 AC-1 7 (2), (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 NIST.800-53.r5 IA-5 (3), 3, 3, 3 (NIST.800-53.r5 SC-13), NIST.800-53.r5 SC-2 (4), NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-7 (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.R5 SI-7 NIST.800-53.r5 SC-8 (6), PCI DSS v4.0.1/4.2.1

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: AWS::CloudFront::Distribution

AWS Config -Regel: [cloudfront-viewer-policy-https](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob eine CloudFront Amazon-Distribution verlangt, dass Zuschauer HTTPS direkt verwenden, oder ob sie eine Umleitung verwendet. Die Steuerung schlägt fehl, wenn sie auf allow-all für defaultCacheBehavior oder für cacheBehaviors gesetzt ViewerProtocolPolicy ist.

HTTPS (TLS) kann verwendet werden, um zu verhindern, dass potenzielle Angreifer person-in-the-middle oder ähnliche Angriffe verwenden, um den Netzwerkverkehr zu belauschen oder zu manipulieren. Nur verschlüsselte Verbindungen über HTTPS (TLS) sollten zugelassen werden. Die Verschlüsselung von Daten während der Übertragung kann die Leistung beeinträchtigen. Sie sollten Ihre Anwendung mit dieser Funktion testen, um das Leistungsprofil und die Auswirkungen von TLS zu verstehen.

Abhilfe

Informationen zum Verschlüsseln einer CloudFront Verteilung während der Übertragung finden Sie unter [HTTPS für die Kommunikation zwischen Zuschauern erforderlich und CloudFront](#) im Amazon CloudFront Developer Guide.

[CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Niedrig

Art der Ressource: AWS::CloudFront::Distribution

AWS Config -Regel: [cloudfront-origin-failover-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob eine CloudFront Amazon-Distribution mit einer Ursprungsgruppe konfiguriert ist, die zwei oder mehr Ursprünge hat.

CloudFront Origin-Failover kann die Verfügbarkeit erhöhen. Origin-Failover leitet den Datenverkehr automatisch an einen sekundären Ursprung weiter, wenn der primäre Ursprung nicht verfügbar ist oder wenn bestimmte HTTP-Antwortstatuscodes zurückgegeben werden.

Abhilfe

Informationen zur Konfiguration des Origin-Failovers für eine CloudFront Distribution finden Sie unter [Creating an Origin Group](#) im Amazon CloudFront Developer Guide.

[CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 (9), NIST.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8), PCI DSS v4.0.1/10.4.2 NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS::CloudFront::Distribution

AWS Config -Regel: [cloudfront-accesslogs-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Serverzugriffsprotokollierung für CloudFront Distributionen aktiviert ist. Die Steuerung schlägt fehl, wenn die Zugriffsprotokollierung für eine Verteilung nicht aktiviert ist. Dieses Steuerelement bewertet nur, ob die Standardprotokollierung (Legacy) für eine Verteilung aktiviert ist.

CloudFront Zugriffsprotokolle enthalten detaillierte Informationen über jede eingehende Benutzeranfrage CloudFront . Jedes Protokoll enthält Informationen wie Datum und Uhrzeit des Eingangs der Anfrage, die IP-Adresse des Betrachters, der die Anfrage gestellt hat, die Quelle der Anfrage und die Portnummer der Anfrage vom Betrachter. Diese Protokolle sind für Anwendungen wie Sicherheits- und Zugriffsprüfungen sowie forensische Untersuchungen nützlich. Weitere Informationen zur Analyse von Zugriffsprotokollen finden Sie unter [CloudFront Amazon-Protokolle abfragen](#) im Amazon Athena-Benutzerhandbuch.

Abhilfe

Informationen zur Konfiguration der Standardprotokollierung (Legacy) für eine CloudFront Distribution finden [Sie unter Standardprotokollierung konfigurieren \(Legacy\)](#) im Amazon CloudFront Developer Guide.

[CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (21), PCI DSS v4.0.1/6.4.2

Kategorie: Schützen > Schutzdienste

Schweregrad: Mittel

Art der Ressource: AWS::CloudFront::Distribution

AWS Config -Regel: [cloudfront-associated-with-waf](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob CloudFront Distributionen entweder AWS WAF Classic oder AWS WAF Web ACLs zugeordnet sind. Das Steuerelement schlägt fehl, wenn die Distribution keiner Web-ACL zugeordnet ist.

AWS WAF ist eine Firewall für Webanwendungen, die zum Schutz von Webanwendungen und APIs vor Angriffen beiträgt. Sie ermöglicht es Ihnen, eine Gruppe von Regeln (eine sogenannte Web-Zugriffskontrollliste oder Web-ACL) zum Zulassen, Blockieren oder Zählen von Webanforderungen basierend auf von Ihnen definierten anpassbaren Web-Sicherheitsregeln und Bedingungen zu konfigurieren. Stellen Sie sicher, dass Ihre CloudFront Distribution mit einer AWS WAF Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Abhilfe

Informationen zum Verknüpfen einer AWS WAF Web-ACL mit einer CloudFront Distribution finden Sie [unter Verwendung AWS WAF zur Zugriffskontrolle auf Ihre Inhalte](#) im Amazon CloudFront Developer Guide.

[CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden

Verwandte Anforderungen: NIST.800-53.r5 AC-1 7 (2), (1) NIST.800-53.r5 AC-4, 2 NIST.800-53.r5 IA-5 (3), 3, 3, 3 (3), NIST.800-53.r5 SC-1 (4), NIST.800-53.r5 SC-2, NIST.800-53.r5 SC-2 (1), (NIST.800-53.r5 SC-12), NIST.800-53.r5 SC-7 NIST.800-53.R5 SI-7 NIST.800-53.r5 SC-8 (6), NIST.800-53.r5 SC-8 NIST.800-171.r2 3.13.15 NIST.800-53.r5 SC-8

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: AWS::CloudFront::Distribution

AWS Config -Regel: [cloudfront-custom-ssl-certificate](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob CloudFront Distributionen die SSL/TLS Standardzertifikate verwenden CloudFront . Diese Kontrolle ist erfolgreich, wenn die CloudFront Verteilung ein benutzerdefiniertes SSL/TLS Zertifikat verwendet. Diese Kontrolle schlägt fehl, wenn die CloudFront Verteilung das SSL/TLS Standardzertifikat verwendet.

Benutzerdefiniert SSL/TLS ermöglichen es Ihren Benutzern, mithilfe alternativer Domainnamen auf Inhalte zuzugreifen. Sie können benutzerdefinierte Zertifikate in AWS Certificate Manager (empfohlen) oder in IAM speichern.

Abhilfe

Informationen zum Hinzufügen eines alternativen Domainnamens für eine CloudFront Distribution mit einem benutzerdefinierten SSL/TLS Zertifikat finden Sie unter [Hinzufügen eines alternativen Domainnamens](#) im Amazon CloudFront Developer Guide.

[CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Niedrig

Art der Ressource: AWS::CloudFront::Distribution

AWS Config -Regel: [cloudfront-sni-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob CloudFront Amazon-Distributionen ein benutzerdefiniertes SSL/TLS Zertifikat verwenden und so konfiguriert sind, dass SNI zur Bearbeitung von HTTPS-Anfragen verwendet wird. Diese Kontrolle schlägt fehl, wenn ein benutzerdefiniertes SSL/TLS Zertifikat zugeordnet ist, die SSL/TLS Unterstützungsmethode jedoch eine dedizierte IP-Adresse ist.

Die Servernamensanzeige (SNI) ist eine Erweiterung des TLS-Protokolls, die in Browsern und Clients unterstützt wird, die nach 2010 veröffentlicht wurden. Wenn Sie so konfigurieren CloudFront , dass HTTPS-Anfragen mithilfe von SNI bedient CloudFront werden, verknüpfen Sie Ihren alternativen Domainnamen mit einer IP-Adresse für jeden Edge-Standort. Sobald ein Viewer Inhalte von Ihnen

durch Senden einer HTTPS-Anforderung abrufen, leitet DNS die Anforderung an die IP-Adresse des korrekten Edge-Standorts weiter. Die IP-Adresse Ihres Domainnamens wird während der SSL/TLS Handshake-Verhandlung festgelegt. Die IP-Adresse ist nicht für Ihre Distribution reserviert.

Abhilfe

Informationen zur Konfiguration einer CloudFront Distribution für die Verwendung von SNI zur Bearbeitung von HTTPS-Anfragen finden Sie unter [Verwenden von SNI zur Bearbeitung von HTTPS-Anfragen \(funktioniert für die meisten Kunden\) im CloudFront Entwicklerhandbuch](#). Informationen zu benutzerdefinierten SSL-Zertifikaten finden Sie unter [Anforderungen für die Verwendung von SSL/TLS Zertifikaten mit](#). CloudFront

[CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln

Verwandte Anforderungen: NIST.800-53.r5 AC-1 7 (2), (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 NIST.800-53.r5 IA-5 (3), 3, 3, 3 (NIST.800-53.r5 SC-13), (4),, NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-7 (2), NIST.800-53.r5 SC-8 NIST.800-53.R5 SI-7 NIST.800-53.r5 SC-8 (6), PCI DSS v4.0.1/4.2.1 NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-8

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: AWS::CloudFront::Distribution

AWS Config -Regel: [cloudfront-traffic-to-origin-encrypted](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob CloudFront Amazon-Distributionen den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln. Diese Kontrolle schlägt bei einer CloudFront Distribution fehl, deren Ursprungsprotokollrichtlinie „Nur HTTP“ zulässt. Diese Kontrolle schlägt auch fehl, wenn die Ursprungsprotokollrichtlinie der Distribution „Match-Viewer“ lautet, während die Viewer-Protokollrichtlinie „Allow-all“ lautet.

HTTPS (TLS) kann verwendet werden, um das Abhören oder Manipulieren des Netzwerkverkehrs zu verhindern. Nur verschlüsselte Verbindungen über HTTPS (TLS) sollten zugelassen werden.

Abhilfe

Informationen zur Aktualisierung der Origin-Protokollrichtlinie, sodass für eine CloudFront Verbindung eine Verschlüsselung erforderlich ist, finden Sie im Amazon CloudFront Developer Guide unter [HTTPS für die Kommunikation zwischen CloudFront und Ihrem benutzerdefinierten Ursprung](#) erforderlich machen.

[CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden

Verwandte Anforderungen: NIST.800-53.r5 AC-1 7 (2), (1) NIST.800-53.r5 AC-4, 2 NIST.800-53.r5 IA-5 (3), 3, 3, (4), (1), NIST.800-53.r5 SC-1 (NIST.800-53.r5 SC-12), NIST.800-53.r5 SC-2 NIST.800-53.R5 SI-7 NIST.800-53.r5 SC-8 (6), NIST.800-53.r5 SC-8 NIST.800-171.r2 3.13.15, PCI DSS v4.0.1/4.2.1 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-8

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: AWS::CloudFront::Distribution

AWS Config -Regel: [cloudfront-no-deprecated-ssl-protocols](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob CloudFront Amazon-Distributionen veraltete SSL-Protokolle für die HTTPS-Kommunikation zwischen CloudFront Edge-Standorten und Ihren benutzerdefinierten Ursprüngen verwenden. Diese Kontrolle schlägt fehl, wenn eine CloudFront Distribution über ein Where Includes verfügtCustomOriginConfig. OriginSslProtocols SSLv3

Im Jahr 2015 gab die Internet Engineering Task Force (IETF) offiziell bekannt, dass SSL 3.0 nicht mehr unterstützt werden sollte, da das Protokoll nicht ausreichend sicher ist. Es wird empfohlen, dass Sie TLSv1 .2 oder höher für die HTTPS-Kommunikation mit Ihren benutzerdefinierten Ursprüngen verwenden.

Abhilfe

Informationen zur Aktualisierung der Origin-SSL-Protokolle für eine CloudFront Distribution finden Sie unter [HTTPS für die Kommunikation zwischen CloudFront und Ihrem benutzerdefinierten Ursprung erforderlich](#) im Amazon CloudFront Developer Guide.

[CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen

Verwandte Anforderungen: NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2), PCI DSS v4.0.1/2.2.6

Kategorie: Identifizieren > Ressourcenkonfiguration

Schweregrad: Hoch

Art der Ressource: AWS::CloudFront::Distribution

AWS Config -Regel: [cloudfront-s3-origin-non-existent-bucket](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob CloudFront Amazon-Distributionen auf nicht existierende Amazon S3-Ursprünge verweisen. Die Kontrolle schlägt bei einer CloudFront Distribution fehl, wenn der Ursprung so konfiguriert ist, dass er auf einen nicht existierenden Bucket verweist. Diese Steuerung gilt nur für CloudFront Distributionen, bei denen ein S3-Bucket ohne statisches Website-Hosting der S3-Ursprung ist.

Wenn eine CloudFront Distribution in Ihrem Konto so konfiguriert ist, dass sie auf einen nicht existierenden Bucket verweist, kann ein böswilliger Dritter den Bucket erstellen, auf den verwiesen wird, und seine eigenen Inhalte über Ihre Distribution bereitstellen. Wir empfehlen, alle Ursprünge unabhängig vom Routing-Verhalten zu überprüfen, um sicherzustellen, dass Ihre Distributionen auf die richtigen Ursprünge verweisen.

Abhilfe

Informationen zum Ändern einer CloudFront Distribution, sodass sie auf einen neuen Ursprung verweist, finden Sie unter [Aktualisieren einer Distribution](#) im Amazon CloudFront Developer Guide.

[CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden

Kategorie: Schützen > Sicheres Zugriffsmanagement > Ressource nicht öffentlich zugänglich

Schweregrad: Mittel

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config -Regel: [cloudfront-s3-origin-access-control-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob für eine CloudFront Amazon-Distribution mit einem Amazon S3-Ursprung die Origin Access Control (OAC) konfiguriert ist. Die Kontrolle schlägt fehl, wenn OAC nicht für die CloudFront Distribution konfiguriert ist.

Wenn Sie einen S3-Bucket als Ursprung für Ihre CloudFront Distribution verwenden, können Sie OAC aktivieren. Dies ermöglicht den Zugriff auf den Inhalt im Bucket nur über die angegebene CloudFront Distribution und verhindert den direkten Zugriff aus dem Bucket oder einer anderen Distribution. Obwohl Origin Access Identity (OAI) CloudFront unterstützt wird, bietet OAC zusätzliche Funktionen, und Distributionen, die OAI verwenden, können zu OAC migriert werden. OAI bietet zwar eine sichere Möglichkeit, auf S3-Ursprünge zuzugreifen, weist jedoch Einschränkungen auf, z. B. mangelnde Unterstützung für detaillierte Richtlinienkonfigurationen und für HTTP/HTTPS Anfragen, die die POST-Methode verwenden und für die Signature Version 4 (Sigv4) erforderlich AWS ist. AWS-Regionen OAI unterstützt auch keine Verschlüsselung mit AWS Key Management Service. OAC basiert auf einer AWS bewährten Methode zur Verwendung von IAM-Dienstprinzipalen zur Authentifizierung mit S3-Ursprüngen.

Abhilfe

Informationen zur Konfiguration von OAC für eine CloudFront Distribution mit S3-Ursprüngen finden Sie unter [Beschränken des Zugriffs auf einen Amazon S3 S3-Ursprung](#) im Amazon CloudFront Developer Guide.

[CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config Regel: `tagged-cloudfront-distribution` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine CloudFront Amazon-Distribution Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind `requiredTagKeys`. Die Steuerung schlägt fehl, wenn die Distribution keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Verteilung mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer CloudFront Distribution finden Sie unter [Tagging CloudFront Amazon-Distributionen](#) im Amazon CloudFront Developer Guide.

[CloudFront.15] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: AWS::CloudFront::Distribution

AWS Config -Regel: [cloudfront-ssl-policy-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:securityPolicies: TLSv1.2_2021 (nicht anpassbar)

Diese Kontrolle prüft, ob eine CloudFront Amazon-Distribution für die Verwendung der empfohlenen TLS-Sicherheitsrichtlinie konfiguriert ist. Die Kontrolle schlägt fehl, wenn die CloudFront Distribution nicht für die Verwendung der empfohlenen TLS-Sicherheitsrichtlinie konfiguriert ist.

Wenn Sie eine CloudFront Amazon-Distribution so konfigurieren, dass Zuschauer HTTPS für den Zugriff auf Inhalte verwenden müssen, müssen Sie eine Sicherheitsrichtlinie auswählen und die zu verwendende SSL/TLS Mindestprotokollversion angeben. Dies bestimmt, welche Protokollversion für die Kommunikation mit Zuschauern CloudFront verwendet wird und welche Chiffren zur Verschlüsselung der Kommunikation CloudFront verwendet werden. Wir empfehlen, die neueste Sicherheitsrichtlinie zu verwenden, die dies bietet. CloudFront Dadurch wird sichergestellt, dass die neuesten Cipher Suites CloudFront verwendet werden, um Daten zu verschlüsseln, die zwischen einem Viewer und einer Distribution übertragen werden. CloudFront

 Note

Dieses Steuerelement generiert Ergebnisse nur für CloudFront Distributionen, die für die Verwendung benutzerdefinierter SSL-Zertifikate konfiguriert sind und die nicht für die Unterstützung älterer Clients konfiguriert sind.

Abhilfe

Informationen zur Konfiguration der Sicherheitsrichtlinie für eine CloudFront Distribution finden Sie unter [Eine Distribution aktualisieren](#) im Amazon CloudFront Developer Guide. Wenn Sie die Sicherheitsrichtlinie für eine Distribution konfigurieren, wählen Sie die neueste Sicherheitsrichtlinie aus.

Security Hub Hub-Kontrollen für AWS CloudTrail

Diese AWS Security Hub Kontrollen bewerten den AWS CloudTrail Service und die Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungseignisse für Lese- und Schreibvorgänge umfasst

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/2.1, CIS AWS Foundations Benchmark v1.4.0/3.1, CIS AWS Foundations Benchmark v3.0.0/3.1, NIST.800-53.r5 AC-2 (4), (26), (9), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 (22) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-14(1), NIST.800-53.r5 CA-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8), NIST.800-53.r5 SA-8

Kategorie: Identifizieren > Protokollierung

Schweregrad: Hoch

Art der Ressource: AWS :: Account

AWS Config -Regel: [multi-region-cloudtrail-enabled](#)

Art des Zeitplans: Periodisch

Parameter:

- `readWriteType`: ALL (nicht anpassbar)
- `includeManagementEvents`: true (nicht anpassbar)

Dieses Steuerelement prüft, ob es mindestens einen multiregionalen AWS CloudTrail Trail gibt, der Lese- und Schreibverwaltungsereignisse erfasst. Das Steuerelement schlägt fehl, wenn es deaktiviert CloudTrail ist oder wenn es nicht mindestens einen CloudTrail Pfad gibt, der Lese- und Schreibverwaltungsereignisse erfasst.

AWS CloudTrail zeichnet AWS API-Aufrufe für Ihr Konto auf und übermittelt Ihnen Protokolldateien. Die aufgezeichneten Informationen beinhalten die folgenden Informationen:

- Identität des API-Aufrufers
- Zeit des API-Aufrufs
- Quell-IP-Adresse des API-Aufrufers
- Anforderungsparameter
- Antwortelemente, die von zurückgegeben wurden AWS-Service

CloudTrail stellt einen Verlauf der AWS API-Aufrufe für ein Konto bereit, einschließlich API-Aufrufen, die über die Befehlszeilentools AWS Management Console AWS SDKs,, getätigt wurden. Die Historie umfasst auch API-Aufrufe von höheren Ebenen, AWS-Services wie z. AWS CloudFormation

Der von erstellte AWS API-Aufrufverlauf CloudTrail ermöglicht Sicherheitsanalysen, die Nachverfolgung von Ressourcenänderungen und die Überprüfung der Einhaltung von Vorschriften. Multi-Regions-Trails bieten auch die folgenden Vorteile.

- Ein Multi-Regions-Trail hilft, unerwartete Aktivitäten zu erkennen, die in ansonsten nicht verwendeten Regionen auftreten.
- Ein Multi-Regions-Trail stellt sicher, dass Global Service Event Logging standardmäßig für einen Trail aktiviert ist. Die globale Protokollierung von Serviceereignissen zeichnet Ereignisse auf, die von AWS globalen Diensten generiert wurden.
- Bei einem Trail mit mehreren Regionen stellen Verwaltungsereignisse für alle Lese- und Schreibvorgänge sicher, dass die Verwaltungsvorgänge für alle Ressourcen in einem CloudTrail AWS-Konto aufgezeichnet werden.

Standardmäßig handelt es sich bei CloudTrail Pfaden, die mit dem AWS Management Console erstellt wurden, um Wanderwege mit mehreren Regionen.

Abhilfe

Informationen zum Erstellen eines neuen Wanderweges mit mehreren Regionen finden Sie unter [Erstellen eines Wanderweges](#) im AWS CloudTrail Benutzerhandbuch. CloudTrail Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Zusätzliche Einstellungen, Protokolldateivalidierung	Aktiviert
Wählen Sie Protokollereignisse, Verwaltungsgereignisse, API-Aktivität	Lesen und Schreiben. Deaktivieren Sie die Kontrollkästchen für Ausschlüsse.

Informationen zum Aktualisieren eines vorhandenen Pfads finden Sie unter [Aktualisieren eines Pfads](#) im AWS CloudTrail Benutzerhandbuch. Wählen Sie unter Verwaltungsgereignisse für API-Aktivität die Optionen Lesen und Schreiben aus.

[CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/2.7, CIS AWS Foundations Benchmark v1.4.0/3.7, CIS AWS Foundations Benchmark v3.0.0/3.5, (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8 NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), (10), NIST.800-53.r5 SI-7 (6), NIST.800-53.r5 SC-7 NIST.800-171.r2 3.3.8, PCI DSS v3.2.1/3.4, PCI DSS v4.0.1/10.3.2 NIST.800-53.r5 SC-2

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: AWS::CloudTrail::Trail

AWS Config -Regel: [cloud-trail-encryption-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement überprüft, CloudTrail ob für die Verwendung der serverseitigen Verschlüsselung (SSE) AWS KMS key konfiguriert ist. Das Steuerelement schlägt fehl, wenn das KmsKeyId nicht definiert ist.

Für eine zusätzliche Sicherheitsebene für Ihre vertraulichen CloudTrail Protokolldateien sollten Sie die [serverseitige Verschlüsselung mit AWS KMS keys \(SSE-KMS\)](#) für Ihre CloudTrail Protokolldateien für die Verschlüsselung im Ruhezustand verwenden. Beachten Sie, dass die von Ihren Buckets gesendeten Protokolldateien standardmäßig durch CloudTrail Amazon mit [serverseitiger Verschlüsselung mit von Amazon S3 verwalteten Verschlüsselungsschlüsseln \(SSE-S3\)](#) verschlüsselt werden.

Abhilfe

Informationen zur Aktivierung der SSE-KMS-Verschlüsselung für CloudTrail Protokolldateien finden Sie unter [Aktualisieren eines Pfads zur Verwendung eines](#) KMS-Schlüssels im Benutzerhandbuch.AWS CloudTrail

[CloudTrail.3] Mindestens ein CloudTrail Trail sollte aktiviert sein

Verwandte Anforderungen: NIST.800-171.R2 3.3.1, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7, PCI DSS v3.2.1/10.1, PCI DSS v3.2.1/10.2.1, PCI DSS v3.2.1/10.2.2, PCI DSS v3.2.1/10.2.3, PCI DSS v3.2.1/10.2.4, PCI DSS v3.2.1/10.2.5, PCI DSS v3.2.1/10.2.6, PCI DSS v3.2.1/10.2.7, PCI DSS v3.2.1/10.3.1, PCI DSS v3.2.1/10.3.2, PCI DSS v3.2.1/10.3.3, PCI DSS v3.2.1/10.3.4, PCI DSS v3.2.1/10.3.5, PCI DSS v3.2.1/10.3.6, PCI DSS v4.0.1/10.2.1

Kategorie: Identifizieren > Protokollierung

Schweregrad: Hoch

Art der Ressource: AWS:::Account

AWS Config -Regel: [cloudtrail-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement überprüft, ob ein AWS CloudTrail -Trail in Ihrem aktiviert ist AWS-Konto. Die Kontrolle schlägt fehl, wenn für Ihr Konto nicht mindestens ein CloudTrail Trail aktiviert ist.

Einige AWS Dienste ermöglichen jedoch nicht die Protokollierung aller APIs Ereignisse. Sie sollten alle zusätzlichen Prüfpfade einrichten, mit CloudTrail Ausnahme der Dokumentation der einzelnen Dienste [CloudTrail unter Unterstützte Dienste und Integrationen](#).

Abhilfe

Informationen zu den ersten CloudTrail Schritten und zur Erstellung eines Trails finden Sie im [AWS CloudTrail Tutorial Erste Schritte mit](#) im AWS CloudTrail Benutzerhandbuch.

[CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/2.2, CIS Foundations Benchmark v1.4.0/3.2, CIS AWS Foundations Benchmark v3.0.0/3.2, NIST.800-53.R5 AU-9, NIST.800-53.R5 SI-4, NIST.800-53.R5 SI-7 (1), NIST.800-53.R5 SI-7 (7), NIST.800-171.r2 3.3.8, PCI DSS v3.2.1/10.5.2, PCI DSS v3.2.1/10.5.5, PCI DSS v4.0.1/10.3.2 AWS

Kategorie: Datenschutz > Datenintegrität

Schweregrad: Niedrig

Art der Ressource: AWS::CloudTrail::Trail

AWS Config -Regel: [cloud-trail-log-file-validation-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement überprüft in einem CloudTrail Trail, ob die Integritätsprüfung der Protokolldatei aktiviert ist.

CloudTrail Bei der Überprüfung der Protokolldatei wird eine digital signierte Digest-Datei erstellt, die einen Hash jedes Protokolls enthält, das in Amazon S3 CloudTrail geschrieben wird. Sie können diese Digestdateien verwenden, um festzustellen, ob eine Protokolldatei nach CloudTrail der Übermittlung des Protokolls geändert, gelöscht oder unverändert geblieben ist.

Security Hub empfiehlt, dass Sie die Dateiüberprüfung auf allen Wegen aktivieren. Die Protokolldateiinvalidierung bietet zusätzliche Integritätsprüfungen von CloudTrail Protokollen.

Abhilfe

Informationen zum Aktivieren der CloudTrail Protokolldateiinvalidierung finden Sie unter [Aktivieren der Überprüfung der Integrität von AWS CloudTrail Protokolldateien CloudTrail](#) im Benutzerhandbuch.

[CloudTrail.5] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden

Verwandte Anforderungen: PCI DSS v3.2.1/10.5.3, CIS AWS Foundations Benchmark v1.2.0/2.4, CIS Foundations Benchmark v1.4.0/3.4, NIST.800-53.r5 AC-2 (4), (26), (9), (9), NIST.800-53.r5 AC-4 NIST.800-53.R5 SI-20, NIST.800-53.r5 AC-6 NIST.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8), Nist.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-4 (20) (5), NIST.800-53.R5 SI-7 (8) AWS NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-6(5), NIST.800-53.r5 AU-7(1), NIST.800-53.r5 CA-7

Kategorie: Identifizieren > Protokollierung

Schweregrad: Niedrig

Art der Ressource: `AWS::CloudTrail::Trail`

AWS Config -Regel: [cloud-trail-cloud-watch-logs-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement überprüft, ob CloudTrail -Trails so konfiguriert sind, dass Protokolle an CloudWatch Protokolle gesendet werden. Die Steuerung schlägt fehl, wenn die `CloudWatchLogsLogGroupArn` Eigenschaft des Trails leer ist.

CloudTrail zeichnet AWS API-Aufrufe auf, die in einem bestimmten Konto getätigt werden. Die aufgezeichneten Informationen beinhalten Folgendes:

- Die Identität des API-Aufrufrers
- Die Uhrzeit des API-Aufrufs
- Die Quell-IP-Adresse des API-Aufrufrers
- Die Anforderungsparametern
- Die Antwortelemente, die von der zurückgegeben wurden AWS-Service

CloudTrail verwendet Amazon S3 für die Speicherung und Lieferung von Protokolldateien. Sie können CloudTrail Protokolle für langfristige Analysen in einem bestimmten S3-Bucket erfassen. Um Echtzeitanalysen durchzuführen, können Sie so konfigurieren, dass CloudWatch Protokolle CloudTrail an Logs gesendet werden.

CloudTrail Sendet bei einem Trail, der in allen Regionen eines Kontos aktiviert ist, Protokolldateien aus all diesen Regionen an eine CloudWatch Logs-Protokollgruppe.

Security Hub empfiehlt, dass Sie CloudTrail CloudWatch Protokolle an Logs senden. Beachten Sie, dass mit dieser Empfehlung sichergestellt werden soll, dass Kontoaktivitäten erfasst, überwacht und entsprechend alarmiert werden. Sie können CloudWatch Logs verwenden, um dies mit Ihrem AWS-Services einzurichten. Diese Empfehlung schließt die Verwendung einer anderen Lösung nicht aus.

Das Senden von CloudTrail CloudWatch Protokollen an Logs ermöglicht die Protokollierung von Aktivitäten in Echtzeit und im Verlauf auf der Grundlage von Benutzer, API, Ressource und IP-Adresse. Mit diesem Ansatz können Sie Alarme und Benachrichtigungen für ungewöhnliche oder sensible Kontoaktivitäten einrichten.

Abhilfe

Informationen zur Integration CloudTrail mit CloudWatch Logs finden Sie im AWS CloudTrail Benutzerhandbuch unter [Ereignisse an CloudWatch Logs senden](#).

[CloudTrail.6] Sicherstellen, dass der S3-Bucket, in dem CloudTrail Protokolle gespeichert werden, nicht öffentlich zugänglich ist

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/2.3, CIS Foundations Benchmark v1.4.0/3.3, PCI DSS AWS v4.0.1/1.4.4

Kategorie: Identifizieren > Protokollierung

Schweregrad: Kritisch

Art der Ressource: AWS::S3::Bucket

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Periodisch und durch Änderung ausgelöst

Parameter: Keine

CloudTrail protokolliert eine Aufzeichnung jedes API-Aufrufs, der in Ihrem Konto getätigt wurde. Diese Protokolldateien werden in einem S3-Bucket gespeichert. CIS empfiehlt, die S3-Bucket-Richtlinie oder Zugriffskontrollliste (ACL) auf den S3-Bucket anzuwenden, der CloudTrail protokolliert, um den öffentlichen Zugriff auf die CloudTrail Protokolle zu verhindern. Wenn der öffentliche Zugriff auf CloudTrail Protokollinhalte gewährt wird, kann dies einem Angreifer dabei helfen, Schwachstellen in der Nutzung oder Konfiguration des betroffenen Kontos zu erkennen.

Um diese Prüfung durchzuführen, verwendet Security Hub zunächst benutzerdefinierte Logik, um nach dem S3-Bucket zu suchen, in dem Ihre CloudTrail Logs gespeichert sind. Anschließend überprüft es anhand der AWS Config verwalteten Regeln, ob der Bucket öffentlich zugänglich ist.

Wenn Sie Ihre Logs in einem einzigen zentralen S3-Bucket zusammenfassen, führt Security Hub die Prüfung nur für das Konto und die Region durch, in der sich der zentrale S3-Bucket befindet. Für andere Konten und Regionen lautet der Kontrollstatus Keine Daten.

Wenn der Bucket öffentlich zugänglich ist, generiert die Prüfung einen Fehlschlag.

Abhilfe

Informationen zum Blockieren des öffentlichen Zugriffs auf Ihren CloudTrail S3-Bucket finden Sie unter [Konfiguration der Einstellungen zum Blockieren des öffentlichen Zugriffs für Ihre S3-Buckets](#) im Amazon Simple Storage Service-Benutzerhandbuch. Wählen Sie alle vier Amazon-S3-Block-Public-Access-Einstellungen aus.

[CloudTrail.7] Sicherstellen, dass die S3-Bucket-Zugriffsprotokollierung für den CloudTrail S3-Bucket aktiviert ist

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/2.6, CIS Foundations Benchmark v1.4.0/3.6, CIS AWS Foundations Benchmark v3.0.0/3.4, PCI DSS AWS v4.0.1/10.2.1

Kategorie: Identifizieren > Protokollierung

Schweregrad: Niedrig

Art der Ressource: AWS::S3::Bucket

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Die S3-Bucket-Zugriffsprotokollierung generiert ein Protokoll, das Zugriffsdatensätze für jede Anfrage an Ihren S3-Bucket enthält. Ein Zugriffsprotokoll-Datensatz enthält Details über jede Anfrage, wie beispielsweise den Anforderungstyp, die in der Anfrage angeforderten Ressource sowie Uhrzeit und Datum der Anfrage.

CIS empfiehlt, die Bucket-Zugriffsprotokollierung für den CloudTrail S3-Bucket zu aktivieren.

Durch das Aktivieren der S3-Bucket-Protokollierung für Ziel-S3-Buckets können Sie alle Ereignisse erfassen, die Auswirkungen auf Objekte in einem Ziel-Bucket haben können. Wenn Protokolle so konfiguriert sind, dass sie in einem separaten Bucket platziert werden, haben Sie Zugang zu Protokollinformationen, die in Sicherheits- und Vorfallreaktions-Workflows hilfreich sein können.

Um diese Prüfung durchzuführen, verwendet Security Hub zunächst benutzerdefinierte Logik, um nach dem Bucket zu suchen, in dem Ihre CloudTrail Protokolle gespeichert sind, und verwendet dann die AWS Config verwaltete Regel, um zu überprüfen, ob die Protokollierung aktiviert ist.

Wenn CloudTrail Protokolldateien von mehreren AWS-Konten in einen einzigen Amazon S3 S3-Ziel-Bucket übertragen werden, wertet Security Hub diese Kontrolle nur anhand des Ziel-Buckets in der Region aus, in der er sich befindet. Dadurch werden Ihre Ergebnisse optimiert. Sie sollten diese Option jedoch CloudTrail in allen Konten aktivieren, die Logs an den Ziel-Bucket senden. Für alle Konten außer dem Konto, das den Ziel-Bucket enthält, lautet der Kontrollstatus Keine Daten.

Abhilfe

Informationen zum Aktivieren der Serverzugriffsprotokollierung für Ihren CloudTrail S3-Bucket finden Sie unter [Aktivieren der Amazon S3 S3-Serverzugriffsprotokollierung](#) im Amazon Simple Storage Service-Benutzerhandbuch.

[CloudTrail.9] CloudTrail Pfade sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::CloudTrail::Trail`

AWS Config Regel: `tagged-cloudtrail-trail` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplanytyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Allowed values	Security Hub Hub-Stand ardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS	No default value

Parameter	Beschreibung	Typ	Allowed values	Security Hub Hub-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen.	

Dieses Steuerelement prüft, ob ein AWS CloudTrail Trail Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn der Trail keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Trail mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `aws:` beginnen, werden ignoriert.

Ein Tag ist eine Markierung, die Sie einer AWS -Ressource zuordnen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Tags können Ihnen helfen, - Ressourcen zu identifizieren, zu organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC — Attribute-based access) als Autorisierungsstrategie implementieren, die Berechtigungen auf der Grundlage von Tags definiert. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und AWS -Ressourcen anfügen. Sie können eine einzelne ABAC-Richtlinie oder einen separaten Richtlinienatz für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen zugelassen werden, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt. Weitere Informationen finden Sie unter [Was ist ABAC für AWS?](#) im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, einschließlich AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem CloudTrail Trail finden Sie [AddTags](#) in der AWS CloudTrail API-Referenz.

[CloudTrail.10] Event-Datenspeicher in CloudTrail Lake sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys

Verwandte Anforderungen: NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-1 2 (2), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-2 8 (1), NIST.800-53.R5 SI-7 (6)

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: AWS::CloudTrail::EventDataStore

AWS Config -Regel: [event-data-store-cmk-encryption-enabled](#)

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Allowed values	Security Hub Hub-Stand ardwert
kmsKeyArns	Eine Liste von Amazon-Re sourcennamen (ARNs) AWS KMS keys , die in die Bewertung aufgenommen werden sollen. Das Steuerele ment generiert einen FAILED	StringList (maximal 3 Elemente)	1—3 ARNs der vorhanden en KMS-Schlü ssel. Beispiel: arn:aws:k ms:us-wes t-2:11112 2223333:k ey/1234ab cd-12ab-3 4cd-56ef-	Kein Standardw ert

Parameter	Beschreibung	Typ	Allowed values	Security Hub Hub-Standardwert
	Befund, wenn ein Ereignisdatenspeicher nicht mit einem KMS-Schlüssel in der Liste verschlüsselt ist.		123456789 0ab .	

Dieses Steuerelement prüft, ob ein AWS CloudTrail Lake-Ereignisdatenspeicher im Ruhezustand verschlüsselt ist, wenn er von einem Kunden verwaltet AWS KMS key wird. Die Steuerung schlägt fehl, wenn der Ereignisdatenspeicher nicht mit einem vom Kunden verwalteten KMS-Schlüssel verschlüsselt ist. Sie können optional eine Liste von KMS-Schlüsseln angeben, die das Steuerelement in die Bewertung einbeziehen soll.

Standardmäßig verschlüsselt AWS CloudTrail Lake Ereignisdatenspeicher mit von Amazon S3 verwalteten Schlüsseln (SSE-S3) unter Verwendung eines AES-256-Algorithmus. Für zusätzliche Kontrolle können Sie CloudTrail Lake so konfigurieren, dass stattdessen ein vom Kunden verwalteter Ereignisdatenspeicher (SSE-KMS) verschlüsselt wird. AWS KMS key Ein vom Kunden verwalteter KMS-Schlüssel ist ein AWS KMS key , den Sie erstellen, besitzen und in Ihrem verwalteten AWS-Konto. Sie haben volle Kontrolle über diesen KMS-Schlüsseltyp. Dazu gehören die Definition und Pflege der Schlüsselrichtlinie, die Verwaltung von Zuschüssen, die Rotation von kryptografischem Material, die Zuweisung von Tags, die Erstellung von Aliasnamen sowie die Aktivierung und Deaktivierung des Schlüssels. Sie können einen vom Kunden verwalteten KMS-Schlüssel für kryptografische Operationen für Ihre CloudTrail Daten verwenden und die Nutzung anhand von Protokollen überprüfen. CloudTrail

Abhilfe

Informationen zum Verschlüsseln eines AWS CloudTrail Lake-Ereignisdatenspeichers mit einem AWS KMS key von Ihnen angegebenen Datenspeicher finden Sie unter [Aktualisieren eines Ereignisdatenspeichers](#) im AWS CloudTrail Benutzerhandbuch. Nachdem Sie einen KMS-Schlüssel einem Ereignisdatenspeicher zugeordnet haben, kann der KMS-Schlüssel nicht entfernt oder geändert werden.

Security Hub Hub-Kontrollen für Amazon CloudWatch

Diese AWS Security Hub Kontrollen bewerten den CloudWatch Service und die Ressourcen von Amazon. Die Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[CloudWatch.1] Für den Benutzer „root“ sollten ein Filter und ein Alarm für die Log-Metrik vorhanden sein

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/1.1, CIS Foundations Benchmark v1.2.0/3.3, CIS AWS Foundations Benchmark v1.4.0/1.7, CIS Foundations Benchmark v1.4.0/4.3, AWS NIST.800-171.R2 3.14.6, NIST.800-171.r2 3.14.7, AWS PCI DSS v3.2.1/7.2.1

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

AWS::Logs::MetricFilterAWS::CloudWatch::AlarmAWS::CloudTrail::TrailRessourcentyp::,
AWS::SNS::Topic

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Der Root-Benutzer hat uneingeschränkten Zugriff auf alle -Services und -Ressourcen in einem AWS-Konto. Wir empfehlen Ihnen dringend, den Root-Benutzer nicht für tägliche Aufgaben zu verwenden. Durch die Minimierung der Nutzung des Root-Benutzers und die Anwendung des Prinzips der geringsten Rechte für die Zugriffsverwaltung wird das Risiko unbeabsichtigter Änderungen und der unbeabsichtigten Offenlegung hochberechtigter Anmeldeinformationen verringert.

Als bewährte Methode sollten Sie Ihre Anmeldeinformationen als Root-Benutzer nur dann verwenden, wenn sie für die [Ausführung von Konto- und Dienstverwaltungsaufgaben](#) erforderlich sind. Wenden Sie AWS Identity and Access Management (IAM-) Richtlinien direkt auf Gruppen und Rollen an, aber nicht auf Benutzer. Ein Tutorial zur Einrichtung eines Administrators für den täglichen Gebrauch finden Sie im [IAM-Benutzerhandbuch unter Erstellen Ihres ersten IAM-Admin-Benutzers und Ihrer ersten Gruppe](#)

Um diese Prüfung durchzuführen, verwendet Security Hub benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 1.7 im [CIS AWS Foundations Benchmark v1.4.0](#)

vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

Note

Wenn Security Hub die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Wanderwege mit mehreren Regionen können sich auch in einer anderen Region befinden.

Die Prüfung führt zu FAILED Ergebnissen in den folgenden Fällen:

- Es ist kein Trail konfiguriert.
- Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von NO_DATA:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

Wir empfehlen Organization Trails, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von NO_DATA für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema

erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub WARNING Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Eine Anleitung finden Sie unter [Erste Schritte mit Amazon SNS](#) im Amazon Simple Notification Service-Entwicklerhandbuch. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter [Erstellen eines Pfads](#).

Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.

3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Metrikfilter für eine Protokollgruppe erstellen](#). Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	<code>{\$.userIdentity.type="Root" && \$.userIdentity.invokedBy NOT EXISTS && \$.eventType != "AwsServiceEvent"}</code>
Metrik-Namespace	LogMetrics
Metrikwert	1
Standardwert	0

4. Einen Alarm basierend auf dem Filter erstellen. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen](#). Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Threshold-Typ	Statisch
Wann immer <i>your-metric-name</i> ist...	Größer/Gleich
als...	1

[CloudWatch.2] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für nicht autorisierte API-Aufrufe vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/3.1, NIST.800-171.R2 3.13.1, NIST.800-171.r2 3.14.6, NIST.800-171.R2 3.14.7

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

AWS::Logs::MetricFilterAWS::CloudWatch::AlarmAWS::CloudTrail::TrailRessourcentyp,,,
AWS::SNS::Topic

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarme einrichten. CloudWatch

CIS empfiehlt Ihnen, einen metrikfilter und einen Alarm für nicht autorisierte API-Aufrufe zu erstellen. Die Überwachung nicht autorisierter API-Aufrufe hilft, Anwendungsfehler aufzudecken, und kann die Erkennung böswilliger Aktivitäten beschleunigen.

Um diese Prüfung durchzuführen, verwendet Security Hub benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 3.1 im [CIS AWS Foundations Benchmark v1.2](#) vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

 Note

Wenn Security Hub die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Wanderwege mit mehreren Regionen können sich auch in einer anderen Region befinden.

Die Prüfung führt zu FAILED Ergebnissen in den folgenden Fällen:

- Es ist kein Trail konfiguriert.
- Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von NO_DATA:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

Wir empfehlen Organization Trails, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von NO_DATA für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. ListSubscriptionsByTopic Andernfalls generiert Security Hub WARNING Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Eine Anleitung finden Sie unter [Erste Schritte mit Amazon SNS](#) im Amazon Simple Notification Service-Entwicklerhandbuch. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter [Erstellen eines Pfads](#).

Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.

3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Metrikfilter für eine Protokollgruppe erstellen](#). Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	<code>{{\$.errorCode="*UnauthorizedOperation"}} {{\$.errorCode="AccessDenied*"}}}</code>
Metrik-Namespace	LogMetrics
Metrikwert	1
Standardwert	0

4. Einen Alarm basierend auf dem Filter erstellen. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen](#). Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Threshold-Typ	Statisch

Feld	Value (Wert)
Wann immer <i>your-metric-name</i> ist...	Größer/Gleich
als...	1

[CloudWatch.3] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für die Anmeldung in der Managementkonsole ohne MFA vorhanden sind

Weitere Anforderungen: CIS AWS Foundations Benchmark v1.2.0/3.2

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Ressourcentyp: AWS::Logs::MetricFilter,, AWS::CloudWatch::Alarm
AWS::CloudTrail::Trail AWS::SNS::Topic

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarmer einrichten. CloudWatch

CIS empfiehlt, einen Metrikfilter und Alarm-Konsolen-Logins zu erstellen, die nicht durch MFA geschützt sind. Durch die Überwachung zur Feststellung von Single-Factor-Konsolenanmeldungen wird die Transparenz im Hinblick auf Konten ohne MFA-Schutz gesteigert.

Um diese Prüfung durchzuführen, verwendet Security Hub benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 3.2 im [CIS AWS Foundations Benchmark v1.2](#) vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

Note

Wenn Security Hub die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um

Organisations-Trails handeln, die zu einem anderen Konto gehören. Wanderwege mit mehreren Regionen können sich auch in einer anderen Region befinden.

Die Prüfung führt zu FAILED Ergebnissen in den folgenden Fällen:

- Es ist kein Trail konfiguriert.
- Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von NO_DATA:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

Wir empfehlen Organization Trails, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von NO_DATA für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. ListSubscriptionsByTopic Andernfalls generiert Security Hub WARNING Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Eine Anleitung finden Sie unter [Erste Schritte mit Amazon SNS](#) im Amazon Simple Notification Service-Entwicklerhandbuch. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter [Erstellen eines Pfads](#).

Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.

3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Metrikfilter für eine Protokollgruppe erstellen](#). Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	<pre>{ (\$.eventName = "ConsoleLogin") && (\$.additionalEventData.MFAUsed != "Yes") && (\$.userIdentity.type = "IAMUser") && (\$.responseElements.ConsoleLogin = "Success") }</pre>
Metrik-Namespace	LogMetrics
Metrikwert	1
Standardwert	0

4. Einen Alarm basierend auf dem Filter erstellen. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen](#). Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Threshold-Typ	Statisch

Feld	Value (Wert)
Wann immer <i>your-metric-name</i> ist...	Größer/Gleich
als...	1

[CloudWatch.4] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der IAM-Richtlinie vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/3.4, CIS Foundations Benchmark v1.4.0/4.4, NIST.800-171.R2 3.14.6, AWS NIST.800-171.R2 3.14.7

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

AWS::Logs::MetricFilterAWS::CloudWatch::AlarmAWS::CloudTrail::TrailRessourcentyp::,,
AWS::SNS::Topic

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob Sie API-Aufrufe in Echtzeit überwachen, indem es CloudTrail CloudWatch Protokolle an Logs weiterleitet und entsprechende Metrikfilter und Alarmer einrichtet.

CIS empfiehlt, einen Metrikfilter und einen Alarm für Änderungen an den IAM-Richtlinien zu erstellen. Die Überwachung dieser Änderungen hilft sicherzustellen, dass Authentifizierungs- und Autorisierungskontrollen intakt bleiben.

Note

Wenn Security Hub die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Wanderwege mit mehreren Regionen können sich auch in einer anderen Region befinden.
Die Prüfung führt zu FAILED Ergebnissen in den folgenden Fällen:

- Es ist kein Trail konfiguriert.
- Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von `NO_DATA`:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

Wir empfehlen Organization Trails, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

Note

Unser empfohlenes Filtermuster für diese Behebungsschritte unterscheidet sich von dem Filtermuster in den CIS-Leitlinien. Unsere empfohlenen Filter zielen nur auf Ereignisse ab, die aus IAM-API-Aufrufen stammen.

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Eine Anleitung finden Sie unter [Erste Schritte mit Amazon SNS](#) im Amazon Simple Notification Service-Entwicklerhandbuch. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter [Erstellen eines Pfads](#).

Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.

3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Metrikfilter für eine Protokollgruppe erstellen](#). Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	<pre>{ (\$.eventSource=iam.amazonaws.com) && ((\$.eventName=DeleteGroupPolicy) (\$.eventName=DeleteRolePolicy) (\$.eventName=DeleteUserPolicy) (\$.eventName=PutGroupPolicy) (\$.eventName=PutRolePolicy) (\$.eventName=PutUserPolicy) (\$.eventName=CreatePolicy) (\$.eventName=DeletePolicy) (\$.eventName=CreatePolicyVersion) (\$.eventName=DeletePolicyVersion) (\$.eventName=AttachRolePolicy) (\$.eventName=DetachRolePolicy) (\$.eventName=AttachUserPolicy) (\$.eventName=DetachUserPolicy)) }</pre>

Feld	Value (Wert)
	<code> (\$.eventName=AttachGroupPolicy) (\$.eventName=DetachGroupPolicy))}</code>
Metrik-Namespace	LogMetrics
Metrikwert	1
Standardwert	0

4. Einen Alarm basierend auf dem Filter erstellen. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen](#). Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Threshold-Typ	Statisch
Wann immer <i>your-metric-name</i> ist...	Größer/Gleich
als...	1

[CloudWatch.5] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für CloudTrail -Config--Config-Änderungen vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/3.5, CIS Foundations Benchmark v1.4.0/4.5, NIST.800-171.R2 3.3.8, AWS NIST.800-171.R2 3.14.6, NIST.800-171.R2 3.14.7

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

AWS::Logs::MetricFilterAWS::CloudWatch::AlarmAWS::CloudTrail::TrailRessourcentyp,,,
AWS::SNS::Topic

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarmer einrichten. CloudWatch

CIS empfiehlt, einen metrischen Filter und einen Alarm für Änderungen an den CloudTrail Konfigurationseinstellungen zu erstellen. Die Überwachung dieser Änderungen hilft sicherzustellen, dass die Transparenz für Aktivitäten in diesem Konto erhalten bleibt.

Um diese Prüfung durchzuführen, verwendet Security Hub benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 4.5 im [CIS AWS Foundations Benchmark v1.4.0](#) vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

Note

Wenn Security Hub die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Wanderwege mit mehreren Regionen können sich auch in einer anderen Region befinden.

Die Prüfung führt zu FAILED Ergebnissen in den folgenden Fällen:

- Es ist kein Trail konfiguriert.
- Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von NO_DATA:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

Wir empfehlen Organization Trails, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten

Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von NO_DATA für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. ListSubscriptionsByTopic Andernfalls generiert Security Hub WARNING Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Eine Anleitung finden Sie unter [Erste Schritte mit Amazon SNS](#) im Amazon Simple Notification Service-Entwicklerhandbuch. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter [Erstellen eines Pfads](#).

Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.

3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Metrikfilter für eine Protokollgruppe erstellen](#). Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	<pre>{{\$.eventName>CreateTrail} {\$.eventName=UpdateTrail} {\$.eventName>DeleteTrail} </pre>

Feld	Value (Wert)
	<code>(\$.eventName=StartLogging) (\$.eventName=StopLogging)}</code>
Metrik-Namespace	LogMetrics
Metrikwert	1
Standardwert	0

4. Einen Alarm basierend auf dem Filter erstellen. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen](#). Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Threshold-Typ	Statisch
Wann immer <i>your-metric-name</i> ist...	Größer/Gleich
als...	1

[CloudWatch.6] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für AWS Management Console Authentifizierungsfehler vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/3.6, CIS Foundations Benchmark v1.4.0/4.6, NIST.800-171.R2 AWS 3.14.6, NIST.800-171.R2 3.14.7

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

AWS::Logs::MetricFilterAWS::CloudWatch::AlarmAWS::CloudTrail::TrailRessourcentyp,,,
AWS::SNS::Topic

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarmer einrichten. CloudWatch

CIS empfiehlt, einen metrischen Filter und einen Alarm für fehlgeschlagene Konsolenauthentifizierungsversuche zu erstellen. Durch die Überwachung fehlgeschlagener Konsolanmeldungen kann die Vorlaufzeit für die Erkennung von Brute-Force-Angriffsversuchen auf Anmeldeinformationen reduziert werden, durch die ein Indikator geliefert werden kann (wie z. B. eine Quell-IP), den Sie in anderen Ereigniskorrelationen verwenden können.

Um diese Prüfung durchzuführen, verwendet Security Hub benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 4.6 im [CIS AWS Foundations Benchmark v1.4.0](#) vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

Note

Wenn Security Hub die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Wanderwege mit mehreren Regionen können sich auch in einer anderen Region befinden.

Die Prüfung führt zu FAILED Ergebnissen in den folgenden Fällen:

- Es ist kein Trail konfiguriert.
- Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von NO_DATA:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

Wir empfehlen Organization Trails, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads

führt zu einem Kontrollstatus von NO_DATA für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub WARNING Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Eine Anleitung finden Sie unter [Erste Schritte mit Amazon SNS](#) im Amazon Simple Notification Service-Entwicklerhandbuch. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter [Erstellen eines Pfads](#).

Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.

3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Metrikfilter für eine Protokollgruppe erstellen](#). Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	<code>{{\$.eventName=ConsoleLogin}&& (\$.errorMessage="Failed authentication")}}</code>

Feld	Value (Wert)
Metrik-Namespace	LogMetrics
Metrikwert	1
Standardwert	0

4. Einen Alarm basierend auf dem Filter erstellen. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen](#). Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Threshold-Typ	Statisch
Wann immer <i>your-metric-name</i> ist...	Größer/Gleich
als...	1

[CloudWatch.7] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden verwalteten Schlüsseln vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/3.7, CIS Foundations Benchmark v1.4.0/4.7, NIST.800-171.R2 3.13.10, AWS NIST.800-171.R2 3.13.16, NIST.800-171.R2 3.14.6, NIST.800-171.R2 3.14.7

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

AWS::Logs::MetricFilterAWS::CloudWatch::AlarmAWS::CloudTrail::TrailRessourcentyp,,,
AWS::SNS::Topic

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarmer einrichten. CloudWatch

CIS empfiehlt, einen Metrikfilter und einen Alarm für vom Kunden verwaltete Schlüssel zu erstellen, deren Status in „Deaktiviert“ oder „Geplantes Löschen“ geändert wurde. Mit deaktivierten oder gelöschten Schlüsseln verschlüsselte Daten sind nicht mehr zugänglich.

Um diese Prüfung durchzuführen, verwendet Security Hub benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 4.7 im [CIS AWS Foundations Benchmark v1.4.0](#) vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden. Die Steuerung schlägt auch fehl, wenn sie `ExcludeManagementEventSources` enthält `kms.amazonaws.com`.

Note

Wenn Security Hub die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Wanderwege mit mehreren Regionen können sich auch in einer anderen Region befinden.

Die Prüfung führt zu FAILED Ergebnissen in den folgenden Fällen:

- Es ist kein Trail konfiguriert.
- Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von `NO_DATA`:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

Wir empfehlen Organization Trails, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von

Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub WARNING Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Eine Anleitung finden Sie unter [Erste Schritte mit Amazon SNS](#) im Amazon Simple Notification Service-Entwicklerhandbuch. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter [Erstellen eines Pfads](#).

Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.

3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Metrikfilter für eine Protokollgruppe erstellen](#). Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	<code>{{\$.eventSource=kms.amazonaws.com) && ((\$.eventName=DisableKey) (\$.eventName=ScheduleKeyDeletion))}}</code>

Feld	Value (Wert)
Metrik-Namespace	LogMetrics
Metrikwert	1
Standardwert	0

4. Einen Alarm basierend auf dem Filter erstellen. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen](#). Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Threshold-Typ	Statisch
Wann immer <i>your-metric-name</i> ist...	Größer/Gleich
als...	1

[CloudWatch.8] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der S3-Bucket-Richtlinie vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/3.8, CIS Foundations Benchmark v1.4.0/4.8, NIST.800-171.R2 AWS 3.14.6, NIST.800-171.R2 3.14.7

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

AWS::Logs::MetricFilterAWS::CloudWatch::AlarmAWS::CloudTrail::TrailRessourcentyp,,
AWS::SNS::Topic

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarmer einrichten. CloudWatch

CIS empfiehlt, einen Metrikfilter und einen Alarm für Änderungen an den S3-Bucket-Richtlinien zu erstellen. Durch das Überwachen dieser Änderungen können Sie die Zeit reduzieren, die zum Erkennen und Korrigieren permissiver Richtlinien für sensible S3-Buckets erforderlich ist.

Um diese Prüfung durchzuführen, verwendet Security Hub benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 4.8 im [CIS AWS Foundations Benchmark v1.4.0](#) vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

Note

Wenn Security Hub die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Wanderwege mit mehreren Regionen können sich auch in einer anderen Region befinden.

Die Prüfung führt zu FAILED Ergebnissen in den folgenden Fällen:

- Es ist kein Trail konfiguriert.
- Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von NO_DATA:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

Wir empfehlen Organization Trails, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von NO_DATA für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie

können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub WARNING Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Eine Anleitung finden Sie unter [Erste Schritte mit Amazon SNS](#) im Amazon Simple Notification Service-Entwicklerhandbuch. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter [Erstellen eines Pfads](#).

Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.

3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Metrikfilter für eine Protokollgruppe erstellen](#). Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	<code>{ (\$.eventSource=s3.amazonaws.com) && ((\$.eventName=PutBucketAcl) (\$.eventName=PutBucketPolicy) (\$.eventName=PutBucketCors) (\$.eventName=PutBucketLifecycle) (\$.eventName=PutBucketReplication) (\$.eventName=Delet</code>

Feld	Value (Wert)
	<code>eBucketPolicy) (\$.eventName=DeleteBucketCors) (\$.eventName=DeleteBucketLifecycle) (\$.eventName=DeleteBucketReplication))}</code>
Metrik-Namespace	LogMetrics
Metrikwert	1
Standardwert	0

4. Einen Alarm basierend auf dem Filter erstellen. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen](#). Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Threshold-Typ	Statisch
Wann immer <i>your-metric-name</i> ist...	Größer/Gleich
als...	1

[CloudWatch.9] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für AWS Config -Config--Config-Änderungen vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/3.9, CIS Foundations Benchmark v1.4.0/4.9, NIST.800-171.R2 3.3.8, AWS NIST.800-171.R2 3.14.6, NIST.800-171.R2 3.14.7

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

AWS::Logs::MetricFilterAWS::CloudWatch::AlarmAWS::CloudTrail::TrailRessourcentyp,,,
AWS::SNS::Topic

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarmer einrichten. CloudWatch

CIS empfiehlt, einen metrischen Filter und einen Alarm für Änderungen an den AWS Config Konfigurationseinstellungen zu erstellen. Die Überwachung dieser Änderungen hilft sicherzustellen, dass die Transparenz im Hinblick auf Konfigurationselemente in diesem Konto erhalten bleibt.

Um diese Prüfung durchzuführen, verwendet Security Hub benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 4.9 im [CIS AWS Foundations Benchmark v1.4.0](#) vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

Note

Wenn Security Hub die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Wanderwege mit mehreren Regionen können sich auch in einer anderen Region befinden.

Die Prüfung führt zu FAILED Ergebnissen in den folgenden Fällen:

- Es ist kein Trail konfiguriert.
- Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von NO_DATA:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

Wir empfehlen Organization Trails, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können

nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von NO_DATA für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub WARNING Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Eine Anleitung finden Sie unter [Erste Schritte mit Amazon SNS](#) im Amazon Simple Notification Service-Entwicklerhandbuch. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter [Erstellen eines Pfads](#).

Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.

3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Metrikfilter für eine Protokollgruppe erstellen](#). Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	<code>{{\$.eventSource=config.amazonaws.com) && (\$.event</code>

Feld	Value (Wert)
	Name=StopConfigurationRecorder) (\$.eventName=DeleteDeliveryChannel) (\$.eventName=PutDeliveryChannel) (\$.eventName=PutConfigurationRecorder))}
Metrik-Namespaces	LogMetrics
Metrikwert	1
Standardwert	0

4. Einen Alarm basierend auf dem Filter erstellen. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen](#). Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Threshold-Typ	Statisch
Wann immer <i>your-metric-name</i> ist...	Größer/Gleich
als...	1

[CloudWatch.10] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Sicherheitsgruppe vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/3.10, CIS Foundations Benchmark v1.4.0/4.10, NIST.800-171.R2 3.14.6, AWS NIST.800-171.R2 3.14.7

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

AWS::Logs::MetricFilter
 AWS::CloudWatch::Alarm
 AWS::CloudTrail::Trail
 Ressourcentyp: AWS::SNS::Topic

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarmer einrichten. CloudWatch Sicherheitsgruppen sind ein zustandsorientierter Paketfilter zur Steuerung von ein- und ausgehendem Datenverkehr in einer VPC.

CIS empfiehlt, einen Metrikfilter und einen Alarm für Änderungen an Sicherheitsgruppen zu erstellen. Die Überwachung dieser Änderungen hilft sicherzustellen, dass -Ressourcen und -Services nicht unbeabsichtigt ungeschützt sind.

Um diese Prüfung durchzuführen, verwendet Security Hub benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Control 4.10 im [CIS AWS Foundations Benchmark v1.4.0](#) vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

Note

Wenn Security Hub die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Wanderwege mit mehreren Regionen können sich auch in einer anderen Region befinden.

Die Prüfung führt zu FAILED Ergebnissen in den folgenden Fällen:

- Es ist kein Trail konfiguriert.
- Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von NO_DATA:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

Wir empfehlen Organization Trails, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von NO_DATA für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. ListSubscriptionsByTopic Andernfalls generiert Security Hub WARNING Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Eine Anleitung finden Sie unter [Erste Schritte mit Amazon SNS](#) im Amazon Simple Notification Service-Entwicklerhandbuch. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter [Erstellen eines Pfads](#).

Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.

3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Metrikfilter für eine Protokollgruppe erstellen](#). Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	<code>{(\$.eventName=AuthorizeSecurityGroupIngress) (\$.eventName=AuthorizeSecurityGroupEgress) (\$.eventName=RevokeSecurityGroupIngress) (\$.eventName=RevokeSecurityGroupEgress) (\$.eventName=CreateSecurityGroup) (\$.eventName>DeleteSecurityGroup)}</code>
Metrik-Namespace	LogMetrics
Metrikwert	1
Standardwert	0

4. Einen Alarm basierend auf dem Filter erstellen. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen](#). Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Threshold-Typ	Statisch
Wann immer <i>your-metric-name</i> ist...	Größer/Gleich
als...	1

[CloudWatch.11] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/3.11, CIS Foundations Benchmark v1.4.0/4.11, NIST.800-171.R2 3.14.6, AWS NIST.800-171.R2 3.14.7

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

`AWS::Logs::MetricFilter``AWS::CloudWatch::Alarm``AWS::CloudTrail::Trail``Ressourcentyp::,`
`AWS::SNS::Topic`

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarmer einrichten. CloudWatch NACLs werden als zustandsloser Paketfilter verwendet, um den eingehenden und ausgehenden Verkehr für Subnetze in einer VPC zu kontrollieren.

CIS empfiehlt, einen Metrikfilter zu erstellen und bei Änderungen an einem Alarm auszulösen. NACLs Durch die Überwachung dieser Änderungen wird sichergestellt, dass AWS Ressourcen und Dienste nicht unbeabsichtigt offengelegt werden.

Um diese Prüfung durchzuführen, verwendet Security Hub benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 4.11 im [CIS AWS Foundations Benchmark v1.4.0](#) vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

Note

Wenn Security Hub die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Wanderwege mit mehreren Regionen können sich auch in einer anderen Region befinden.

Die Prüfung führt zu FAILED Ergebnissen in den folgenden Fällen:

- Es ist kein Trail konfiguriert.
- Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von `NO_DATA`:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

Wir empfehlen Organization Trails, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Eine Anleitung finden Sie unter [Erste Schritte mit Amazon SNS](#) im Amazon Simple Notification Service-Entwicklerhandbuch. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter [Erstellen eines Pfads](#).

Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.

- Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Metrikfilter für eine Protokollgruppe erstellen](#). Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	<code>{(\$.eventName=CreateNetworkAcl) (\$.eventName=CreateNetworkAclEntry) (\$.eventName>DeleteNetworkAcl) (\$.eventName>DeleteNetworkAclEntry) (\$.eventName=ReplaceNetworkAclEntry) (\$.eventName=ReplaceNetworkAclAssociation)}</code>
Metrik-Namespace	LogMetrics
Metrikwert	1
Standardwert	0

- Einen Alarm basierend auf dem Filter erstellen. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen](#). Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Threshold-Typ	Statisch
Wann immer <i>your-metric-name</i> ist...	Größer/Gleich
als...	1

[CloudWatch.12] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an Network-Gateways vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/3.12, CIS Foundations Benchmark v1.4.0/4.12, NIST.800-171.R2 3.3.1, AWS NIST.800-171.R2 3.13.1

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

AWS::Logs::MetricFilterAWS::CloudWatch::AlarmAWS::CloudTrail::TrailRessourcentyp,,,
AWS::SNS::Topic

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarmer einrichten. CloudWatch Netzwerk-Gateways sind erforderlich, um Datenverkehr an ein Ziel außerhalb einer VPC zu senden und Datenverkehr von einem solchen Ziel zu empfangen.

CIS empfiehlt Ihnen, einen metrikfilter und einen Alarm für Änderungen an Network-Gateways zu erstellen. Die Überwachung dieser Änderungen hilft sicherzustellen, dass der gesamte eingehende und ausgehende Datenverkehr die VPC-Grenze über einen kontrollierten Pfad durchquert.

Um diese Prüfung durchzuführen, verwendet Security Hub benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 4.12 im [CIS AWS Foundations Benchmark v1.2](#) vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

Note

Wenn Security Hub die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Wanderwege mit mehreren Regionen können sich auch in einer anderen Region befinden.

Die Prüfung führt zu FAILED Ergebnissen in den folgenden Fällen:

- Es ist kein Trail konfiguriert.
- Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von NO_DATA:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

Wir empfehlen Organization Trails, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von NO_DATA für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. ListSubscriptionsByTopic Andernfalls generiert Security Hub WARNING Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Eine Anleitung finden Sie unter [Erste Schritte mit Amazon SNS](#) im Amazon Simple Notification Service-Entwicklerhandbuch. Erstellen Sie ein

Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.

- Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter [Erstellen eines Pfads](#).

Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.

- Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Metrikfilter für eine Protokollgruppe erstellen](#). Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	<code>{ (\$.eventName=CreateCustomerGateway) (\$.eventName>DeleteCustomerGateway) (\$.eventName=AttachInternetGateway) (\$.eventName>CreateInternetGateway) (\$.eventName>DeleteInternetGateway) (\$.eventName=DetachInternetGateway)}</code>
Metrik-Namespaces	LogMetrics
Metrikwert	1
Standardwert	0

- Einen Alarm basierend auf dem Filter erstellen. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen](#). Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Threshold-Typ	Statisch
Wann immer <i>your-metric-name</i> ist...	Größer/Gleich

Feld	Value (Wert)
als...	1

[CloudWatch.13] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Routing-Tabelle vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/3.13, CIS Foundations Benchmark v1.4.0/4.13, NIST.800-171.R2 3.3.1, AWS NIST.800-171.R2 3.13.1, NIST.800-171.R2 3.14.6, NIST.800-171.R2 3.14.7

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

AWS::Logs::MetricFilterAWS::CloudWatch::AlarmAWS::CloudTrail::TrailRessourcentyp,,,
AWS::SNS::Topic

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob Sie API-Aufrufe in Echtzeit überwachen, indem es CloudTrail CloudWatch Protokolle an Logs weiterleitet und entsprechende Metrikfilter und Alarmer einrichtet. Routing-Tabellen leiten Netzwerkdatenverkehr zwischen Subnetzen und Netzwerk-Gateways weiter.

CIS empfiehlt, einen Metrikfilter und einen Alarm für Änderungen an Routing-Tabellen zu erstellen. Die Überwachung dieser Änderungen hilft sicherzustellen, dass sämtlicher VPC-Datenverkehr durch einen erwarteten Pfad fließt.

Note

Wenn Security Hub die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Wanderwege mit mehreren Regionen können sich auch in einer anderen Region befinden. Die Prüfung führt zu FAILED Ergebnissen in den folgenden Fällen:

- Es ist kein Trail konfiguriert.
- Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von `NO_DATA`:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

Wir empfehlen Organization Trails, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

Note

Unser empfohlenes Filtermuster für diese Behebungsschritte unterscheidet sich von dem Filtermuster in den CIS-Leitlinien. Unsere empfohlenen Filter zielen nur auf Ereignisse ab, die von Amazon Elastic Compute Cloud (EC2) API-Aufrufen stammen.

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Eine Anleitung finden Sie unter [Erste Schritte mit Amazon SNS](#) im Amazon Simple Notification Service-Entwicklerhandbuch. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter [Erstellen eines Pfads](#).

Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.

3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Metrikfilter für eine Protokollgruppe erstellen](#). Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	<code>{ (\$.eventSource=ec2.amazonaws.com) && ((\$.eventName=CreateRoute) (\$.eventName=CreateRouteTable) (\$.eventName=ReplaceRoute) (\$.eventName=ReplaceRouteTableAssociation) (\$.eventName>DeleteRouteTable) (\$.eventName>DeleteRoute) (\$.eventName=DisassociateRouteTable)) }</code>
Metrik-Namespace	LogMetrics
Metrikwert	1
Standardwert	0

4. Einen Alarm basierend auf dem Filter erstellen. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen](#). Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Threshold-Typ	Statisch
Wann immer <i>your-metric-name</i> ist...	Größer/Gleich
als...	1

[CloudWatch.14] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für VPC-Änderungen vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/3.14, CIS Foundations Benchmark v1.4.0/4.14, NIST.800-171.R2 3.3.1, AWS NIST.800-171.r2 3.13.1, NIST.800-171.R2 3.14.6, NIST.800-171.R2 3.14.7

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

AWS::Logs::MetricFilterAWS::CloudWatch::AlarmAWS::CloudTrail::TrailRessourcentyp,,,
AWS::SNS::Topic

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarmer einrichten. CloudWatch Sie können mehr als eine VPC in einem Konto haben und Sie können eine Peer-Verbindung zwischen zwei herstellen VPCs, sodass der Netzwerkverkehr zwischen VPCs ihnen weitergeleitet werden kann.

CIS empfiehlt, dass Sie einen metrischen Filter und einen Alarm für Änderungen an VPCs erstellen. Die Überwachung dieser Änderungen hilft sicherzustellen, dass Authentifizierungs- und Autorisierungskontrollen intakt bleiben.

Um diese Prüfung durchzuführen, verwendet Security Hub benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 4.14 im [CIS AWS Foundations Benchmark v1.4.0](#)

vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

Note

Wenn Security Hub die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Wanderwege mit mehreren Regionen können sich auch in einer anderen Region befinden.

Die Prüfung führt zu FAILED Ergebnissen in den folgenden Fällen:

- Es ist kein Trail konfiguriert.
- Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von NO_DATA:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

Wir empfehlen Organization Trails, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von NO_DATA für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema

erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub WARNING Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Eine Anleitung finden Sie unter [Erste Schritte mit Amazon SNS](#) im Amazon Simple Notification Service-Entwicklerhandbuch. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter [Erstellen eines Pfads](#).

Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.

3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Metrikfilter für eine Protokollgruppe erstellen](#). Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	<pre>{{\$.eventName=CreateVpc} {\$.eventName>DeleteVpc} {\$.eventName=ModifyVpcAttri bute} {\$.eventName=Accep tVpcPeeringConnection} {\$.eventName=CreateVpcPeeri ngConnection} {\$.eventN ame>DeleteVpcPeeringConnect ion} {\$.eventName=Rejec tVpcPeeringConnection} {\$.eventName=AttachClassicL inkVpc} {\$.eventName=Detac hClassicLinkVpc} {\$.eventN</pre>

Feld	Value (Wert)
	ame=DisableVpcClassicLink) (\$.eventName=EnableVpcClassicLink)}
Metrik-Namespace	LogMetrics
Metrikwert	1
Standardwert	0

4. Einen Alarm basierend auf dem Filter erstellen. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen](#). Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Threshold-Typ	Statisch
Wann immer <i>your-metric-name</i> ist...	Größer/Gleich
als...	1

[CloudWatch.15] Für CloudWatch Alarmer sollten bestimmte Aktionen konfiguriert sein

Verwandte Anforderungen: NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(5), NIST.800-53.r5 CA-7, NIST.800-53.R5 IR-4 (1), NIST.800-53.R5 IR-4 (5), NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-20, NIST.800-53.R5 SI-4 (12), NIST.800-53.R5 SI-4 (5), NIST.800-171.R2 3.3.4, NIST.800-171.R2 3,14.6

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Hoch

Art der Ressource: AWS::CloudWatch::Alarm

AWS Config Regel: [cloudwatch-alarm-action-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>alarmActionRequired</code>	Die Steuerung ermittelt, PASSED ob der Parameter auf eingestellt ist <code>true</code> und ob der Alarm eine Aktion ausführt, wenn der Alarmstatus zu wechseltALARM.	Boolesch	Nicht anpassbar	<code>true</code>
<code>insufficientDataActionRequired</code>	Die Steuerung ermittelt, PASSED ob der Parameter auf eingestellt ist <code>true</code> und ob der Alarm eine Aktion ausführt, wenn der Alarmstatus zu wechseltINSUFFICIENT_DATA .	Boolesch	<code>true</code> oder <code>false</code>	<code>false</code>
<code>okActionRequired</code>	Die Steuerung gibt einen PASSED Befund aus, wenn der Parameter auf eingestellt ist <code>true</code> und der Alarm eine Aktion ausführt, wenn sich der Alarmstatus auf ändertOK.	Boolesch	<code>true</code> oder <code>false</code>	<code>false</code>

Dieses Steuerelement prüft, ob für einen CloudWatch Amazon-Alarm mindestens eine Aktion für den ALARM Status konfiguriert ist. Die Steuerung schlägt fehl, wenn für den Alarm keine Aktion für den ALARM Status konfiguriert ist. Optional können Sie benutzerdefinierte Parameterwerte angeben, sodass auch Alarmaktionen für die OK Zustände INSUFFICIENT_DATA oder erforderlich sind.

Note

Security Hub bewertet diese Kontrolle auf der Grundlage CloudWatch metrischer Alarmer. Metrische Alarmer können Teil von zusammengesetzten Alarmen sein, für die die

angegebenen Aktionen konfiguriert sind. Die Steuerung generiert FAILED Ergebnisse in den folgenden Fällen:

- Die angegebenen Aktionen sind nicht für einen metrischen Alarm konfiguriert.
- Der metrische Alarm ist Teil eines zusammengesetzten Alarms, für den die angegebenen Aktionen konfiguriert sind.

Diese Steuerung konzentriert sich darauf, ob für einen CloudWatch Alarm eine Alarmaktion konfiguriert ist, wohingegen sich [CloudWatch.17](#) auf den Aktivierungsstatus einer CloudWatch Alarmaktion konzentriert.

Wir empfehlen CloudWatch Alarmaktionen, um Sie automatisch zu benachrichtigen, wenn eine überwachte Metrik den definierten Schwellenwert überschreitet. Mithilfe von Überwachungsalarmen können Sie ungewöhnliche Aktivitäten erkennen und schnell auf Sicherheits- und Betriebsprobleme reagieren, wenn ein Alarm in einen bestimmten Zustand übergeht. Die häufigste Art von Alarmaktion besteht darin, einen oder mehrere Benutzer zu benachrichtigen, indem sie eine Nachricht an ein Thema des Amazon Simple Notification Service (Amazon SNS) senden.

Abhilfe

Informationen zu Aktionen, die von CloudWatch Alarmen unterstützt werden, finden Sie unter [Alarmaktionen](#) im CloudWatch Amazon-Benutzerhandbuch.

[CloudWatch.16] CloudWatch Protokollgruppen sollten für einen bestimmten Zeitraum aufbewahrt werden

Kategorie: Identifizieren > Protokollierung

Verwandte Anforderungen: NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-11, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-12

Schweregrad: Mittel

Art der Ressource: AWS : : Logs : : LogGroup

AWS Config Regel: [cw-loggroup-retention-period-check](#)

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Standardwert	
minRetentionTime	Minimaler Aufbewahrungszeitraum in Tagen für CloudWatch Protokollgruppen	Enum	365, 400, 545, 731, 1827, 3653	365	

Diese Kontrolle prüft, ob eine CloudWatch Amazon-Protokollgruppe eine Aufbewahrungsfrist von mindestens der angegebenen Anzahl von Tagen hat. Die Kontrolle schlägt fehl, wenn die Aufbewahrungsdauer kürzer ist als angegeben. Sofern Sie keinen benutzerdefinierten Parameterwert für den Aufbewahrungszeitraum angeben, verwendet Security Hub einen Standardwert von 365 Tagen.

CloudWatch Protokolle zentralisieren die Protokolle von allen Systemen, Anwendungen und AWS-Services in einem einzigen, hochgradig skalierbaren Service. Sie können CloudWatch Logs zur Überwachung, Speicherung und für den Zugriff auf Ihre Protokolldateien aus Amazon-Elastic-Compute-Cloud-Instances (EC2) AWS CloudTrail, Amazon Route 53 und anderen Quellen verwenden. Wenn Sie Ihre Protokolle mindestens ein Jahr lang aufbewahren, können Sie die Aufbewahrungsstandards für Protokolle einhalten.

Abhilfe

Informationen zur Konfiguration der Protokollaufbewahrungseinstellungen finden Sie unter [Ändern der Aufbewahrung von Protokolldaten in CloudWatch Logs](#) im CloudWatch Amazon-Benutzerhandbuch.

[CloudWatch.17] CloudWatch Alarmaktionen sollten aktiviert sein

Kategorie: Erkennung > Erkennungsservices

Verwandte Anforderungen: NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(5), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-4 (12)

Schweregrad: Hoch

Art der Ressource: `AWS::CloudWatch::Alarm`

AWS Config Regel: [cloudwatch-alarm-action-enabled-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob CloudWatch Alarmaktionen aktiviert sind (ActionEnabled sollte auf true gesetzt sein). Die Steuerung schlägt fehl, wenn die Alarmaktion für einen CloudWatch Alarm deaktiviert ist.

 Note

Security Hub bewertet diese Kontrolle auf der Grundlage CloudWatch metrischer Alarme. Metrische Alarme können Teil von zusammengesetzten Alarms sein, bei denen die Alarmaktionen aktiviert sind. Die Steuerung generiert FAILED Ergebnisse in den folgenden Fällen:

- Die angegebenen Aktionen sind nicht für einen metrischen Alarm konfiguriert.
- Der metrische Alarm ist Teil eines zusammengesetzten Alarms, für den Alarmaktionen aktiviert sind.

Diese Steuerung konzentriert sich auf den Aktivierungsstatus einer CloudWatch Alarmaktion, wohingegen sich [CloudWatch.15](#) darauf konzentriert, ob eine ALARM Aktion in einem CloudWatch Alarm konfiguriert ist.

Alarmaktionen benachrichtigen Sie automatisch, wenn eine überwachte Metrik den definierten Schwellenwert überschreitet. Wenn die Alarmaktion deaktiviert ist, werden keine Aktionen ausgeführt, wenn sich der Status des Alarms ändert, und Sie werden nicht über Änderungen der überwachten Messwerte informiert. Wir empfehlen, CloudWatch Alarmaktionen zu aktivieren, damit Sie schnell auf Sicherheits- und Betriebsprobleme reagieren können.

Abhilfe

Um eine CloudWatch Alarmaktion zu aktivieren (Konsole)

1. Öffnen Sie die CloudWatch Konsole unter <https://console.aws.amazon.com/cloudwatch/>.

2. Wählen Sie im Navigationsbereich unter Alarme die Option Alle Alarme aus.
3. Wählen Sie den Alarm, für den Sie Aktionen aktivieren möchten.
4. Wählen Sie für Aktionen die Option Alarmaktionen — neu und dann Aktivieren aus.

Weitere Informationen zur Aktivierung von CloudWatch Alarmaktionen finden Sie unter [Alarmaktionen](#) im CloudWatch Amazon-Benutzerhandbuch.

Security Hub-Steuerungen für CodeArtifact

Diese Security Hub-Steuerelemente bewerten den AWS CodeArtifact Service und die Ressourcen.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[CodeArtifact.1] CodeArtifact Repositorien sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::CodeArtifact::Repository`

AWS Config Regel: `tagged-codeartifact-repository` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS CodeArtifact Repository Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn das Repository keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Repository mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem CodeArtifact Repository finden Sie unter [Markieren eines Repositories CodeArtifact im AWS CodeArtifact](#) Benutzerhandbuch.

Security Hub-Steuerungen für CodeBuild

Diese Security Hub-Steuerelemente bewerten den AWS CodeBuild Service und die Ressourcen.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[CodeBuild.1] Das CodeBuild Bitbucket-Quell-Repository URLs sollte keine vertraulichen Anmeldeinformationen enthalten

Verwandte Anforderungen: NIST.800-53.r5 SA-3, PCI DSS v3.2.1/8.2.1, PCI DSS v4.0.1/8.3.2

Kategorie: Schutz > Sichere Entwicklung

Schweregrad: Kritisch

Art der Ressource: AWS::CodeBuild::Project

AWS Config -Regel: [codebuild-project-source-repo-url-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die URL AWS CodeBuild des Bitbucket-Quell-Repositorys eines Projekts persönliche Zugriffstoken oder einen Benutzernamen und ein Passwort enthält. Die Kontrolle schlägt fehl, wenn die URL des Bitbucket-Quell-Repositorys persönliche Zugriffstoken oder einen Benutzernamen und ein Passwort enthält.

 Note

Dieses Steuerelement bewertet sowohl die Primärquelle als auch die Sekundärquellen eines CodeBuild Build-Projekts. Weitere Informationen zu Projektquellen finden Sie im AWS CodeBuild Benutzerhandbuch unter [Beispiel für mehrere Eingabequellen und Ausgabeartefakte](#).

Anmeldeinformationen sollten nicht im Klartext gespeichert oder übertragen werden oder in der Quell-Repository-URL erscheinen. Statt persönlicher Zugriffstoken oder Anmeldedaten solltest du auf deinen Quellenanbieter zugreifen und deine Quell-Repository-URL so ändern CodeBuild, dass sie nur den Pfad zum Bitbucket-Repository-Speicherort enthält. Die Verwendung persönlicher Zugriffstoken oder Anmeldedaten könnte zu unbeabsichtigter Offenlegung von Daten oder unberechtigtem Zugriff führen.

Abhilfe

Sie können Ihr CodeBuild Projekt aktualisieren, um es zu verwenden. OAuth

Um das persönliche Zugriffstoken für die Standardauthentifizierung/(GitHub) aus der CodeBuild Projektquelle zu entfernen

1. Öffnen Sie die CodeBuild Konsole unter <https://console.aws.amazon.com/codebuild/>.
2. Wählen Sie das Build-Projekt aus, das persönliche Zugriffstoken oder einen Benutzernamen und ein Passwort enthält.
3. Wählen Sie unter Edit (Bearbeiten) die Option Source (Quelle) aus.
4. Wähle Disconnect from GitHub //Bitbucket aus.
5. Wähle Connect using OAuth und dann Connect to GitHub//Bitbucket.
6. Wenn Sie dazu aufgefordert werden, wählen Sie Autorisieren entsprechend aus.
7. Konfigurieren Sie Ihre Repository-URL und zusätzliche Konfigurationseinstellungen nach Bedarf neu.
8. Wählen Sie Update source (Quelle aktualisieren) aus.

Weitere Informationen findest du in den [CodeBuild Anwendungsbeispielen](#) im AWS CodeBuild Benutzerhandbuch.

[CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten

Verwandte Anforderungen: NIST.800-53.r5 IA-5 (7), PCI DSS v3.2.1/8.2.1 NIST.800-53.r5 SA-3, PCI DSS v4.0.1/8.3.2

Kategorie: Schutz > Sichere Entwicklung

Schweregrad: Kritisch

Art der Ressource: AWS::CodeBuild::Project

AWS Config -Regel: [codebuild-project-envvar-awscred-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob das Projekt die Umgebungsvariablen `AWS_ACCESS_KEY_ID` und `AWS_SECRET_ACCESS_KEY` enthält.

Die Anmeldeinformationen für die Authentifizierung `AWS_ACCESS_KEY_ID` und `AWS_SECRET_ACCESS_KEY` sollten niemals in Klartext gespeichert werden, da dies zu einer unbeabsichtigten Datenoffenlegung und unbefugtem Zugriff führen kann.

Abhilfe

Informationen zum Entfernen von Umgebungsvariablen aus einem CodeBuild Projekt finden Sie [AWS CodeBuild im AWS CodeBuild Benutzerhandbuch unter Ändern der Einstellungen eines Build-Projekts](#). Stellen Sie sicher, dass nichts für Umgebungsvariablen ausgewählt ist.

Sie können Umgebungsvariablen mit sensiblen Werten im AWS Systems Manager Parameterspeicher speichern oder AWS Secrets Manager sie dann aus Ihrer Build-Spezifikation abrufen. Anweisungen finden Sie im AWS CodeBuild Benutzerhandbuch im Feld „Wichtig“ [im Abschnitt „Umgebung“](#).

[CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.R5 NIST.800-53.r5 SC-2 SI-7 (6), PCI DSS v4.0.1/10.3.2

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Niedrig

Art der Ressource: `AWS::CodeBuild::Project`

AWS Config -Regel: [codebuild-project-s3-logs-encrypted](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob Amazon S3 S3-Protokolle für ein AWS CodeBuild Projekt verschlüsselt sind. Die Kontrolle schlägt fehl, wenn die Verschlüsselung für S3-Protokolle für ein CodeBuild Projekt deaktiviert ist.

Die Verschlüsselung von Daten im Ruhezustand ist eine empfohlene bewährte Methode, um Ihre Daten um eine Ebene der Zugriffsverwaltung zu erweitern. Durch die Verschlüsselung der Protokolle

im Ruhezustand AWS wird das Risiko verringert, dass ein Benutzer, der sich nicht authentifiziert hat, auf die auf der Festplatte gespeicherten Daten zugreift. Es fügt weitere Zugriffskontrollen hinzu, um den Zugriff nicht autorisierter Benutzer auf die Daten einzuschränken.

Abhilfe

Informationen zum Ändern der Verschlüsselungseinstellungen für CodeBuild Projekt-S3-Protokolle finden Sie [AWS CodeBuild im AWS CodeBuild Benutzerhandbuch unter Ändern der Einstellungen eines Build-Projekts](#).

[CodeBuild1.4] CodeBuild Projektumgebungen sollten eine AWS Config Protokollierungsdauer haben

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (12), (4), NIST.800-53.r5 AC-2 (26), (9), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 NIST.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-9(7), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-4, NIST.800-53.R5 SI-4 (20), NIST.800-53.r5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Ressourcentyp: AWS::CodeBuild::Project

AWS Config -Regel: [codebuild-project-logging-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine CodeBuild Projektumgebung über mindestens eine Protokolloption verfügt, entweder für S3 oder ob CloudWatch Protokolle aktiviert sind. Dieses Steuerelement schlägt fehl, wenn in einer CodeBuild Projektumgebung nicht mindestens eine Protokolloption aktiviert ist.

Aus Sicherheitsgründen ist die Protokollierung eine wichtige Funktion, um future forensische Maßnahmen im Falle von Sicherheitsvorfällen zu ermöglichen. Die Korrelation von Anomalien in CodeBuild Projekten mit Bedrohungserkennungen kann das Vertrauen in die Genauigkeit dieser Bedrohungserkennungen erhöhen.

Abhilfe

Weitere Informationen zur Konfiguration der CodeBuild Projektprotokolleinstellungen finden Sie im Benutzerhandbuch unter [Erstellen eines Build-Projekts \(Konsole\)](#). CodeBuild

[CodeBuild.5] In CodeBuild Projektumgebungen sollte der privilegierte Modus nicht aktiviert sein

Important

Security Hub hat diese Kontrolle im April 2024 eingestellt. Weitere Informationen finden Sie unter [Änderungsprotokoll für Security Hub CSPM-Steuerelemente](#).

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (10), NIST.800-53.r5 AC-6 (2)

Kategorie: Schützen > Sicheres Zugriffsmanagement

Schweregrad: Hoch

Art der Ressource: AWS::CodeBuild::Project

AWS Config -Regel: [codebuild-project-environment-privileged-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob in einer AWS CodeBuild Projektumgebung der privilegierte Modus aktiviert oder deaktiviert ist. Die Steuerung schlägt fehl, wenn in einer CodeBuild Projektumgebung der privilegierte Modus aktiviert ist.

Standardmäßig erlauben Docker-Container keinen Zugriff auf Geräte. Der privilegierte Modus gewährt dem Docker-Container eines Build-Projekts Zugriff auf alle Geräte. Die Einstellung `privilegedMode` mit einem Wert `true` ermöglicht es dem Docker-Daemon, in einem Docker-Container ausgeführt zu werden. Der Docker-Daemon wartet auf Docker-API-Anfragen und verwaltet Docker-Objekte wie Images, Container, Netzwerke und Volumes. Dieser Parameter sollte nur auf `true` gesetzt werden, wenn das Build-Projekt zum Erstellen von Docker-Images verwendet wird.

Andernfalls sollte diese Einstellung deaktiviert werden, um einen unbeabsichtigten Zugriff auf Docker APIs sowie auf die dem Container zugrunde liegende Hardware zu verhindern. Die Einstellung `privilegedMode` auf `false` trägt dazu bei, kritische Ressourcen vor Manipulation und Löschung zu schützen.

Abhilfe

Informationen zum Konfigurieren der Einstellungen für die CodeBuild Projektumgebung finden [Sie im CodeBuild Benutzerhandbuch unter Erstellen eines Build-Projekts \(Konsole\)](#). Wählen Sie im Abschnitt Umgebung nicht die Einstellung Privilegiert aus.

[CodeBuild.7] Exporte von CodeBuild Berichtsgruppen sollten im Ruhezustand verschlüsselt werden

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: `AWS::CodeBuild::ReportGroup`

AWS Config -Regel: [codebuild-report-group-encrypted-at-rest](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Testergebnisse einer AWS CodeBuild Berichtsgruppe, die in einen Amazon Simple Storage Service (Amazon S3) -Bucket exportiert werden, im Ruhezustand verschlüsselt sind. Die Kontrolle schlägt fehl, wenn der Export der Berichtsgruppe im Ruhezustand nicht verschlüsselt ist.

Daten im Ruhezustand beziehen sich auf Daten, die für einen beliebigen Zeitraum in einem persistenten, nichtflüchtigen Speicher gespeichert werden. Durch die Verschlüsselung ruhender Daten können Sie deren Vertraulichkeit schützen, wodurch das Risiko verringert wird, dass ein nicht autorisierter Benutzer darauf zugreifen kann.

Abhilfe

Informationen zur Verschlüsselung des Exports von Berichtsgruppen nach S3 finden Sie unter [Aktualisieren einer Berichtsgruppe](#) im AWS CodeBuild Benutzerhandbuch.

Security Hub-Steuerelemente für Amazon CodeGuru Profiler

Diese Security Hub Hub-Kontrollen bewerten den Service und die Ressourcen von Amazon CodeGuru Profiler.

Diese Kontrollen sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[CodeGuruProfiler.1] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::CodeGuruProfiler::ProfilingGroup`

AWS Config -Regel: `codeguruprofiler-profiling-group-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon CodeGuru Profiler-Profiling-Gruppe Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind. `requiredKeyTags` Die Kontrolle schlägt fehl, wenn die Profiling-Gruppe keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat. `requiredKeyTags` Wenn der Parameter

`requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Profilerstellungsgruppe mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer CodeGuru Profiler-Profiling-Gruppe finden Sie unter [Tagging Profiling Groups](#) im Amazon CodeGuru Profiler-Benutzerhandbuch.

Security Hub-Steuerelemente für Amazon CodeGuru Reviewer

Diese Security Hub Hub-Kontrollen bewerten den Service und die Ressourcen von Amazon CodeGuru Reviewer.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[CodeGuruReviewer.1] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::CodeGuruReviewer::RepositoryAssociation`

AWS Config -Regel: `codegurureviewer-repository-association-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon CodeGuru Reviewer-Repository-Zuordnung Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind `requiredKeyTags`. Die Kontrolle schlägt fehl, wenn die Repository-Zuordnung keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält `requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Repository-Zuordnung mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck,

Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer CodeGuru Reviewer-Repository-Verknüpfung finden Sie unter [Markieren einer Repository-Verknüpfung](#) im Amazon CodeGuru Reviewer-Benutzerhandbuch.

Security Hub-Steuerelemente für Amazon Cognito

Diese AWS Security Hub Kontrollen bewerten den Service und die Ressourcen von Amazon Cognito. Die Steuerelemente sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[Cognito.1] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Ressourcentyp: `AWS::Cognito::UserPool`

AWS Config -Regel: [cognito-user-pool-advanced-security-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
SecurityMode	Der Modus zur Durchsetzung des Bedrohungsschutzes, nach dem das Steuerelement sucht.	String	AUDIT, ENFORCED	ENFORCED

Diese Kontrolle prüft, ob in einem Amazon Cognito Cognito-Benutzerpool der Bedrohungsschutz aktiviert ist und der Erzwingungsmodus für die Standardauthentifizierung auf Vollfunktion eingestellt ist. Die Kontrolle schlägt fehl, wenn der Bedrohungsschutz für den Benutzerpool deaktiviert ist oder wenn der Erzwingungsmodus für die Standardauthentifizierung nicht auf volle Funktionalität eingestellt ist. Sofern Sie keine benutzerdefinierten Parameterwerte angeben, verwendet Security Hub den Standardwert für den Erzwingungsmodus, der ENFORCED für die Standardauthentifizierung auf Vollfunktion gesetzt ist.

Nachdem Sie einen Amazon Cognito Cognito-Benutzerpool erstellt haben, können Sie den Bedrohungsschutz aktivieren und die Maßnahmen anpassen, die als Reaktion auf verschiedene Risiken ergriffen werden. Oder Sie können den Überwachungsmodus verwenden, um Metriken zu erkannten Risiken zu sammeln, ohne Sicherheitsmaßnahmen ergreifen zu müssen. Im Auditmodus veröffentlicht Threat Protection Kennzahlen an Amazon CloudWatch. Sie können Metriken sehen, nachdem Amazon Cognito sein erstes Ereignis generiert hat.

Abhilfe

Informationen zur Aktivierung des Bedrohungsschutzes für einen Amazon Cognito-Benutzerpool finden Sie unter [Erweiterte Sicherheit mit Bedrohungsschutz](#) im Amazon Cognito Developer Guide.

[Cognito.2] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen

Kategorie: Schützen > Sichere Zugriffsverwaltung > Passwortlose Authentifizierung

Schweregrad: Mittel

Art der Ressource: `AWS::Cognito::IdentityPool`

AWS Config -Regel: [cognito-identity-pool-unauth-access-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon Cognito Cognito-Identitätspool so konfiguriert ist, dass er nicht authentifizierte Identitäten zulässt. Die Kontrolle schlägt fehl, wenn der Gastzugriff für den Identitätspool aktiviert ist (der `AllowUnauthenticatedIdentities` Parameter ist auf `gesetzttrue`).

Wenn ein Amazon Cognito Cognito-Identitätspool nicht authentifizierte Identitäten zulässt, stellt der Identitätspool temporäre AWS Anmeldeinformationen für Benutzer bereit, die sich nicht über einen Identitätsanbieter authentifiziert haben (Gäste). Dies birgt Sicherheitsrisiken, da es anonymen Zugriff auf Ressourcen ermöglicht. AWS Wenn Sie den Gastzugriff deaktivieren, können Sie sicherstellen, dass nur ordnungsgemäß authentifizierte Benutzer auf Ihre AWS Ressourcen zugreifen können, wodurch das Risiko eines unbefugten Zugriffs und potenzieller Sicherheitsverletzungen verringert wird. Als bewährte Methode sollte ein Identitätspool die Authentifizierung durch unterstützte Identitätsanbieter erfordern. Wenn ein nicht authentifizierter Zugriff erforderlich ist, ist es wichtig, die Berechtigungen für nicht authentifizierte Identitäten sorgfältig einzuschränken und deren Verwendung regelmäßig zu überprüfen und zu überwachen.

Abhilfe

Informationen zur Deaktivierung des Gastzugriffs für einen Amazon Cognito-Identitätspool finden Sie unter [Gastzugriff aktivieren oder deaktivieren](#) im Amazon Cognito Developer Guide.

Security Hub-Steuerungen für AWS Config

Diese Security Hub-Steuerelemente bewerten den AWS Config Service und die Ressourcen.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[Config.1] AWS Config sollte aktiviert sein und die serviceverknüpfte Rolle für die Ressourcenaufzeichnung verwenden

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/2.5, CIS Foundations Benchmark v1.4.0/3.5, CIS AWS Foundations Benchmark v3.0.0/3.3, NIST.800-53.R5 CM-3, NIST.800-53.R5 CM-6 (1), NIST.800-53.R5 CM-8, NIST.800-53.R5 CM-8 (2), PCI DSS v3.2.1/10.5.2, PCI DSS v3.2.1/11.5 AWS

Kategorie: Identifizieren > Bestand

Schweregrad: Kritisch

Art der Ressource: AWS :: Account

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
includeConfigServiceLinkedRoleCheck	Das Steuerelement bewertet nicht, ob die serviceverknüpfte Rolle AWS Config verwendet wird, wenn der Parameter auf false gesetzt ist.	Boolesch	true oder false	true

Dieses Steuerelement prüft, ob AWS Config es in Ihrem Konto aktuell aktiviert ist AWS-Region, zeichnet alle Ressourcen auf, die den in der aktuellen Region aktivierten Kontrollen entsprechen, und verwendet die [dienstverknüpfte Rolle AWS Config](#). Der Name der dienstbezogenen Rolle lautet. AWSServiceRoleForConfig Wenn Sie die dienstgebundene Rolle nicht verwenden und den includeConfigServiceLinkedRoleCheck Parameter nicht auf setzen, schlägt die Steuerung

fehlfalſe, da andere Rollen möglicherweise nicht über die erforderlichen Berechtigungen verfügen, AWS Config um Ihre Ressourcen korrekt aufzuzeichnen.

Der AWS Config Dienst führt die Konfigurationsverwaltung der unterstützten AWS Ressourcen in Ihrem Konto durch und übermittelt Ihnen Protokolldateien. Zu den aufgezeichneten Informationen gehören das Konfigurationselement (AWS Ressource), Beziehungen zwischen Konfigurationselementen und alle Konfigurationsänderungen innerhalb von Ressourcen. Globale Ressourcen sind Ressourcen, die in jeder Region verfügbar sind.

Die Kontrolle wird wie folgt bewertet:

- Wenn die aktuelle Region als Ihre [Aggregationsregion](#) festgelegt ist, liefert das Steuerelement nur PASSED Ergebnisse, wenn globale AWS Identity and Access Management (IAM-) Ressourcen aufgezeichnet werden (sofern Sie Steuerelemente aktiviert haben, für die diese erforderlich sind).
- Wenn die aktuelle Region als verknüpfte Region festgelegt ist, bewertet das Steuerelement nicht, ob globale IAM-Ressourcen aufgezeichnet wurden.
- Wenn die aktuelle Region nicht in Ihrem Aggregator enthalten ist oder wenn in Ihrem Konto keine regionsübergreifende Aggregation eingerichtet ist, liefert das Steuerelement nur dann PASSED Ergebnisse, wenn globale IAM-Ressourcen aufgezeichnet werden (sofern Sie Steuerelemente aktiviert haben, die diese erfordern).

Die Kontrollergebnisse werden nicht davon beeinflusst, ob Sie sich für die tägliche oder kontinuierliche Aufzeichnung von Änderungen des Ressourcenstatus in entscheiden. AWS Config Die Ergebnisse dieser Steuerung können sich jedoch ändern, wenn neue Steuerelemente veröffentlicht werden, wenn Sie die automatische Aktivierung neuer Steuerelemente konfiguriert haben oder über eine zentrale Konfigurationsrichtlinie verfügen, die neue Kontrollen automatisch aktiviert. Wenn Sie in diesen Fällen nicht alle Ressourcen aufzeichnen, müssen Sie die Aufzeichnung für Ressourcen konfigurieren, die neuen Steuerelementen zugeordnet sind, um ein PASSED Ergebnis zu erhalten.

Security Hub-Sicherheitsprüfungen funktionieren nur dann wie vorgesehen, wenn Sie sie AWS Config in allen Regionen aktivieren und die Ressourcenaufzeichnung für Kontrollen konfigurieren, die dies erfordern.

 Note

Config.1 setzt voraus, dass dies in allen Regionen aktiviert AWS Config ist, in denen Sie Security Hub verwenden.

Da es sich bei Security Hub um einen regionalen Dienst handelt, wird bei der für dieses Steuerelement durchgeführten Prüfung nur die aktuelle Region für das Konto ausgewertet. Um Sicherheitsüberprüfungen anhand globaler IAM-Ressourcen in einer Region zuzulassen, müssen Sie globale IAM-Ressourcen in dieser Region aufzeichnen. Regionen, in denen keine globalen IAM-Ressourcen erfasst sind, erhalten eine PASSED Standardbewertung für Kontrollen, die globale IAM-Ressourcen überprüfen. Da globale IAM-Ressourcen überall identisch sind, empfehlen wir AWS-Regionen, globale IAM-Ressourcen nur in der Heimatregion aufzuzeichnen (sofern die regionsübergreifende Aggregation in Ihrem Konto aktiviert ist). IAM-Ressourcen werden nur in der Region aufgezeichnet, in der die globale Ressourcenaufzeichnung aktiviert ist.

Bei den global aufgezeichneten IAM-Ressourcentypen, die AWS Config unterstützt werden, handelt es sich um IAM-Benutzer, -Gruppen, -Rollen und vom Kunden verwaltete Richtlinien. Sie können erwägen, Security Hub-Steuerelemente, die diese Ressourcentypen überprüfen, in Regionen zu deaktivieren, in denen die globale Ressourcenaufzeichnung deaktiviert ist. Weitere Informationen finden Sie unter [Vorgeschlagene Steuerelemente zur Deaktivierung in Security Hub CSPM](#).

Abhilfe

Erfassen Sie in der Heimatregion und in Regionen, die nicht Teil eines Aggregators sind, alle Ressourcen, die für Kontrollen erforderlich sind, die in der aktuellen Region aktiviert sind, einschließlich globaler IAM-Ressourcen, falls Sie Steuerungen aktiviert haben, die globale IAM-Ressourcen erfordern.

In verknüpften Regionen können Sie einen beliebigen AWS Config Aufnahmemodus verwenden, sofern Sie alle Ressourcen aufzeichnen, die den Steuerelementen entsprechen, die in der aktuellen Region aktiviert sind. Wenn Sie in verknüpften Regionen Steuerelemente aktiviert haben, die die Aufzeichnung globaler IAM-Ressourcen erfordern, erhalten Sie kein FAILED Ergebnis (Ihre Aufzeichnung anderer Ressourcen ist ausreichend).

Anhand des StatusReasons Felds im Compliance Objekt Ihrer Suche können Sie feststellen, warum Sie für dieses Steuerelement einen Fehler gefunden haben. Weitere Informationen finden Sie unter [Einzelheiten zur Einhaltung der Kontrollbestimmungen](#).

Eine Liste der Ressourcen, die für jedes Steuerelement aufgezeichnet werden müssen, finden Sie unter [Erforderliche AWS Config Ressourcen für Kontrollbefunde](#). Allgemeine Informationen zur

Aktivierung AWS Config und Konfiguration der Ressourcenaufzeichnung finden Sie unter [Aktivierung und Konfiguration AWS Config für Security Hub CSPM](#).

Security Hub-Steuerelemente für Amazon Connect

Diese Security Hub Hub-Kontrollen bewerten den Service und die Ressourcen von Amazon Connect.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[Connect.1] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::CustomerProfiles::ObjectType`

AWS Config -Regel: `customerprofiles-object-type-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon Connect Connect-Objekttyp für Kundenprofile Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind `requiredKeyTags`. Die Steuerung schlägt fehl, wenn der Objekttyp keine Tag-Schlüssel hat oder wenn er nicht

alle im Parameter angegebenen Schlüssel hat `requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Objekttyp mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Objekttyp „Kundenprofile“ finden [Sie unter Hinzufügen von Tags zu Ressourcen in Amazon Connect](#) im Amazon Connect Connect-Administratorhandbuch.

[Connect.2] Für Amazon Connect Connect-Instances sollte die Protokollierung aktiviert sein CloudWatch

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Ressourcentyp: AWS::Connect::Instance

AWS Config -Regel: [connect-instance-logging-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob eine Amazon Connect Connect-Instance so konfiguriert ist, dass sie Flow-Protokolle in einer CloudWatch Amazon-Protokollgruppe generiert und speichert. Die Steuerung schlägt fehl, wenn die Amazon Connect Connect-Instance nicht für die Generierung und Speicherung von Flow-Protokollen in einer CloudWatch Protokollgruppe konfiguriert ist.

Amazon Connect Connect-Flow-Logs bieten Echtzeitdetails zu Ereignissen in Amazon Connect Connect-Flows. Ein Flow definiert das Kundenerlebnis mit einem Amazon Connect Connect-Kontaktzentrum von Anfang bis Ende. Wenn Sie eine neue Amazon Connect Connect-Instance erstellen, wird standardmäßig automatisch eine CloudWatch Amazon-Protokollgruppe erstellt, um Flow-Logs für die Instance zu speichern. Mithilfe von Flow-Protokollen können Sie Abläufe analysieren, Fehler finden und Betriebsmetriken überwachen. Sie können auch Benachrichtigungen für bestimmte Ereignisse einrichten, die in einem Flow auftreten können.

Abhilfe

Informationen zur Aktivierung von Flow-Logs für eine Amazon Connect Connect-Instance finden Sie unter [Amazon Connect Connect-Flow-Logs in einer CloudWatch Amazon-Protokollgruppe aktivieren](#) im Amazon Connect-Administratorhandbuch.

Security Hub-Steuerelemente für Amazon Data Firehose

Diese Security Hub Hub-Kontrollen bewerten den Service und die Ressourcen von Amazon Data Firehose.

Diese Kontrollen sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 AC-3, NIST.800-53.r5 AU-3, NIST.800-53.r5 SC-1 2, NIST.800-53.r5 SC-1 3, 8 NIST.800-53.r5 SC-2

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: `AWS::KinesisFirehose::DeliveryStream`

AWS Config -Regel: [kinesis-firehose-delivery-stream-encrypted](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon Data Firehose-Lieferstream im Ruhezustand mit serverseitiger Verschlüsselung verschlüsselt ist. Diese Steuerung schlägt fehl, wenn ein Firehose-Lieferstream im Ruhezustand nicht mit serverseitiger Verschlüsselung verschlüsselt ist.

Die serverseitige Verschlüsselung ist eine Funktion in Amazon Data Firehose-Lieferströmen, die Daten automatisch verschlüsselt, bevor sie gespeichert werden, indem ein in AWS Key Management Service () erstellter Schlüssel verwendet wird. AWS KMS Daten werden verschlüsselt, bevor sie in die Data Firehose-Stream-Speicherschicht geschrieben werden, und entschlüsselt, nachdem sie aus dem Speicher abgerufen werden. Auf diese Weise können Sie die gesetzlichen Anforderungen erfüllen und die Sicherheit Ihrer Daten verbessern.

Abhilfe

Informationen zur Aktivierung der serverseitigen Verschlüsselung für Firehose-Lieferstreams finden Sie unter [Datenschutz in Amazon Data Firehose](#) im Amazon Data Firehose Developer Guide.

Security Hub-Steuerungen für AWS DataSync

Diese Security Hub-Steuerelemente bewerten den AWS DataSync Service und die Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[DataSync.1] Für DataSync Aufgaben sollte die Protokollierung aktiviert sein

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Ressourcentyp: `AWS::DataSync::Task`

AWS Config -Regel: [datasync-task-logging-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für eine AWS DataSync Aufgabe die Protokollierung aktiviert ist. Das Steuerelement schlägt fehl, wenn für die Aufgabe die Protokollierung nicht aktiviert ist.

In Auditprotokollen werden Systemaktivitäten verfolgt und überwacht. Sie bieten eine Aufzeichnung von Ereignissen, anhand derer Sie Sicherheitsverletzungen erkennen, Vorfälle untersuchen und Vorschriften einhalten können. Auditprotokolle verbessern auch die allgemeine Rechenschaftspflicht und Transparenz Ihres Unternehmens.

Abhilfe

Informationen zur Konfiguration der Protokollierung für AWS DataSync Aufgaben finden Sie unter [Überwachen von Datenübertragungen mit Amazon CloudWatch Logs](#) im AWS DataSync Benutzerhandbuch.

[DataSync.2] DataSync Aufgaben sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Taggen

Schweregrad: Niedrig

Art der Ressource: AWS::DataSync::Task

AWS Config -Regel: [datasync-task-tagged](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Standardwert
requiredKeyTags	Eine Liste der Tag-Schlüssel vom Typ „“, die einer ausgewerteten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert

zwischen Groß- und Kleinschreibung unterschieden.

Dieses Steuerelement prüft, ob eine AWS DataSync Aufgabe über die im `requiredKeyTags` Parameter angegebenen Tag-Schlüssel verfügt. Das Steuerelement schlägt fehl, wenn die Aufgabe über keine Tagschlüssel oder nicht über alle im `requiredKeyTags` Parameter angegebenen Schlüssel verfügt. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Aufgabe keine Tagschlüssel hat. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws :` Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im [Tagging AWS Resources and Tag Editor User Guide](#).

Note

Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Stichwörtern zu einer AWS DataSync Aufgabe finden Sie unter [Taggen Ihrer AWS DataSync Aufgaben](#) im AWS DataSync Benutzerhandbuch.

Security Hub-Steuerelemente für Amazon Detective

Diese AWS Security Hub Kontrolle bewertet den Service und die Ressourcen von Amazon Detective. Das Steuerelement ist möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[Detective.1] Verhaltensdiagramme von Detektiven sollten markiert werden

Kategorie: Identifizieren > Inventar > Kennzeichnung

Schweregrad: Niedrig

Art der Ressource: `AWS::Detective::Graph`

AWS Config Regel: `tagged-detective-graph` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob ein Amazon Detective-Verhaltensdiagramm Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind `requiredTagKeys`. Das Steuerelement schlägt fehl, wenn das Verhaltensdiagramm keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel enthält `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Verhaltensdiagramm mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Verhaltensdiagramm von Detective finden Sie unter [Hinzufügen von Tags zu einem Verhaltensdiagramm](#) im Amazon Detective Administration Guide.

Security Hub-Steuerungen für AWS DMS

Diese Security Hub-Steuerelemente bewerten den AWS Database Migration Service (AWS DMS) Service und die Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[DMS.1] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, PCI DSS v4.0.1/1.4.4

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Kritisch

Art der Ressource: AWS::DMS::ReplicationInstance

AWS Config -Regel: [dms-replication-not-public](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob AWS DMS Replikationsinstanzen öffentlich sind. Zu diesem Zweck untersucht es den Wert des PubliclyAccessible Felds.

Eine private Replikationsinstanz hat eine private IP-Adresse, auf die Sie außerhalb des Replikationsnetzwerks nicht zugreifen können. Eine Replikationsinstanz sollte eine private IP-Adresse haben, wenn sich die Quell- und Zieldatenbank im selben Netzwerk befinden. Das Netzwerk muss auch über ein VPN oder VPC-Peering mit der VPC der Replikationsinstanz verbunden sein. AWS Direct Connect Weitere Informationen zu öffentlichen und privaten Replikationsinstanzen finden Sie im Benutzerhandbuch unter [Öffentliche und private Replikationsinstanzen](#). AWS Database Migration Service

Sie sollten außerdem sicherstellen, dass der Zugriff auf Ihre AWS DMS Instanzkonfiguration nur autorisierten Benutzern vorbehalten ist. Um dies zu tun, schränken Sie die IAM-Berechtigungen der Benutzer ein, um AWS DMS Einstellungen und Ressourcen zu ändern.

Abhilfe

Sie können die Einstellung für den öffentlichen Zugriff für eine DMS-Replikationsinstanz nicht ändern, nachdem Sie sie erstellt haben. Um die Einstellung für den öffentlichen Zugriff zu ändern, [löschen Sie](#)

[Ihre aktuelle Instanz](#) und [erstellen Sie sie anschließend neu](#). Wählen Sie nicht die Option Öffentlich zugänglich aus.

[DMS.2] DMS-Zertifikate sollten gekennzeichnet sein

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::DMS::Certificate

AWS Config Regel: tagged-dms-certificate (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
requiredTagKeys	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob ein AWS DMS Zertifikat Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn das Zertifikat keine Tagschlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel enthält `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Zertifikat mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `aws:` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck,

Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem DMS-Zertifikat finden Sie unter [Ressourcen kennzeichnen AWS Database Migration Service im Benutzerhandbuch](#).AWS Database Migration Service

[DMS.3] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::DMS::EventSubscription

AWS Config Regel: tagged-dms-eventsubscription (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob ein AWS DMS Ereignisabonnement Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn das Ereignisabonnement keine Tagschlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel enthält `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Ereignisabonnement mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem DMS-Veranstaltungsabonnement finden Sie [AWS Database Migration Service im Benutzerhandbuch unter Ressourcen taggen](#).AWS Database Migration Service

[DMS.4] DMS-Replikationsinstanzen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::DMS::ReplicationInstance

AWS Config Regel: tagged-dms-replicationinstance (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
requiredTagKeys	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob eine AWS DMS Replikationsinstanz über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn die Replikationsinstanz keine Tagschlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Replikationsinstanz mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` , werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer DMS-Replikationsinstanz finden Sie unter [Ressourcen taggen AWS Database Migration Service im Benutzerhandbuch](#).AWS Database Migration Service

[DMS.5] Subnetzgruppen für die DMS-Replikation sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::DMS::ReplicationSubnetGroup`

AWS Config Regel: `tagged-dms-replicationsubnetgroup` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob eine AWS DMS Replikationssubnetzgruppe Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind. `requiredTagKeys` Die Steuerung schlägt fehl, wenn die Replikationssubnetzgruppe keine Tagschlüssel hat oder wenn nicht alle im Parameter angegebenen Schlüssel vorhanden sind. `requiredTagKeys` Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Replikationssubnetzgruppe mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern

verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer DMS-Replikationssubnetzgruppe finden Sie unter [Ressourcen kennzeichnen im AWS Database Migration Service Benutzerhandbuch](#).AWS Database Migration Service

[DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), NIST.800-53.R5 SI-2 (5), PCI DSS v4.0.1/6.3.3

Kategorie: Identifizieren > Sicherheitslücken-, Patch- und Versionsverwaltung

Schweregrad: Mittel

Art der Ressource: AWS::DMS::ReplicationInstance

AWS Config -Regel: [dms-auto-minor-version-upgrade-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob das automatische Upgrade einer Nebenversion für eine AWS DMS Replikationsinstanz aktiviert ist. Die Steuerung schlägt fehl, wenn das automatische Upgrade der Nebenversion für eine DMS-Replikationsinstanz nicht aktiviert ist.

DMS bietet ein automatisches Upgrade der Nebenversionen für jede unterstützte Replikationsengine, sodass Sie Ihre Replikationsinstanz behalten können. up-to-date Nebenversionen können neue Softwarefunktionen, Bugfixes, Sicherheitspatches und Leistungsverbesserungen einführen. Durch die Aktivierung des automatischen Upgrades für kleinere Versionen auf DMS-Replikationsinstanzen werden kleinere Upgrades automatisch während des Wartungsfensters oder sofort angewendet, wenn die Option Änderungen sofort anwenden ausgewählt ist.

Abhilfe

Informationen zur Aktivierung des automatischen Upgrades für Nebenversionen auf DMS-Replikationsinstanzen finden Sie unter [Ändern einer Replikationsinstanz](#) im AWS Database Migration Service Benutzerhandbuch.

[DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 (9), NIST.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8), PCI DSS v4.0.1/10.4.2

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Ressourcentyp: AWS::DMS::ReplicationTask

AWS Config -Regel: [dms-replication-task-targetdb-logging](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Protokollierung mit dem Mindestschweregrad `LOGGER_SEVERITY_DEFAULT` für DMS-Replikationsaufgaben `TARGET_APPLY` und `TARGET_LOAD`

aktiviert ist. Die Steuerung schlägt fehl, wenn die Protokollierung für diese Aufgaben nicht aktiviert ist oder wenn der Mindestschweregrad unter `LOGGER_SEVERITY_DEFAULT` liegt.

DMS verwendet Amazon CloudWatch, um Informationen während des Migrationsprozesses zu protokollieren. Mithilfe der Einstellungen für die Protokollierungsaufgabe können Sie angeben, welche Komponentenaktivitäten protokolliert werden und wie viele Informationen protokolliert werden. Sie sollten die Protokollierung für die folgenden Aufgaben angeben:

- `TARGET_APPLY` – Daten und Data Definition Language (DDL)-Anweisungen werden auf die Zieldatenbank angewendet.
- `TARGET_LOAD` – Daten werden in die Zieldatenbank geladen.

Die Protokollierung spielt bei DMS-Replikationsaufgaben eine entscheidende Rolle, da sie Überwachung, Problembehandlung, Prüfung, Leistungsanalyse, Fehlererkennung und -wiederherstellung sowie historische Analysen und Berichte ermöglicht. Es trägt dazu bei, die erfolgreiche Replikation von Daten zwischen Datenbanken sicherzustellen und gleichzeitig die Datenintegrität und die Einhaltung gesetzlicher Anforderungen zu gewährleisten. Andere Protokollierungsstufen als `DEFAULT` werden für diese Komponenten bei der Problembehandlung selten benötigt. Wir empfehlen, die Protokollierungsebene `DEFAULT` für diese Komponenten beizubehalten, es sei denn, Sie werden ausdrücklich aufgefordert, sie zu ändern Support. Eine minimale Protokollierungsebene von `DEFAULT` stellt sicher, dass Informationsmeldungen, Warnungen und Fehlermeldungen in die Protokolle geschrieben werden. Dieses Steuerelement prüft, ob für die vorangegangenen Replikationsaufgaben mindestens eine der folgenden Protokollierungsstufen gilt: `LOGGER_SEVERITY_DEFAULT`, `LOGGER_SEVERITY_DEBUG`, oder `LOGGER_SEVERITY_DETAILED_DEBUG`.

Abhilfe

Informationen zum Aktivieren der Protokollierung für DMS-Replikationsaufgaben in der Zieldatenbank finden Sie unter [AWS DMS Task-Logs anzeigen und verwalten](#) im AWS Database Migration Service Benutzerhandbuch.

[DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 (9), NIST.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5

AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8), PCI DSS v4.0.1/10.4.2

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Ressourcentyp: AWS::DMS::ReplicationTask

AWS Config -Regel: [dms-replication-task-sourcedb-logging](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Protokollierung mit dem Mindestschweregrad `LOGGER_SEVERITY_DEFAULT` für DMS-Replikationsaufgaben `SOURCE_CAPTURE` und `SOURCE_UNLOAD` aktiviert ist. Die Steuerung schlägt fehl, wenn die Protokollierung für diese Aufgaben nicht aktiviert ist oder wenn der Mindestschweregrad unter `LOGGER_SEVERITY_DEFAULT` liegt.

DMS verwendet Amazon CloudWatch , um Informationen während des Migrationsprozesses zu protokollieren. Mithilfe der Einstellungen für die Protokollierungsaufgabe können Sie angeben, welche Komponentenaktivitäten protokolliert werden und wie viele Informationen protokolliert werden. Sie sollten die Protokollierung für die folgenden Aufgaben angeben:

- `SOURCE_CAPTURE`— Laufende Replikations- oder CDC-Daten (Change Data Capture) werden aus der Quelldatenbank oder dem Quelldienst erfasst und an die `SORTER` Servicekomponente weitergegeben.
- `SOURCE_UNLOAD`— Daten werden bei Volllast aus der Quelldatenbank oder dem Quelldienst entladen.

Die Protokollierung spielt bei DMS-Replikationsaufgaben eine entscheidende Rolle, da sie Überwachung, Fehlerbehebung, Prüfung, Leistungsanalyse, Fehlererkennung und Wiederherstellung sowie historische Analysen und Berichte ermöglicht. Es trägt dazu bei, die erfolgreiche Replikation von Daten zwischen Datenbanken sicherzustellen und gleichzeitig die Datenintegrität und die Einhaltung gesetzlicher Anforderungen zu gewährleisten. Andere Protokollierungsstufen als `DEFAULT` werden für diese Komponenten bei der Problembehandlung selten benötigt. Wir empfehlen, die Protokollierungsebene `DEFAULT` für diese Komponenten

beizubehalten, es sei denn, Sie werden ausdrücklich aufgefordert, sie zu ändern Support. Eine minimale Protokollierungsebene von DEFAULT stellt sicher, dass Informationsmeldungen, Warnungen und Fehlermeldungen in die Protokolle geschrieben werden. Dieses Steuerelement prüft, ob für die vorangegangenen Replikationsaufgaben mindestens eine der folgenden Protokollierungsstufen gilt: `LOGGER_SEVERITY_DEFAULT`, `LOGGER_SEVERITY_DEBUG`, oder `LOGGER_SEVERITY_DETAILED_DEBUG`.

Abhilfe

Informationen zum Aktivieren der Protokollierung für DMS-Replikationsaufgaben in der Quelldatenbank finden Sie unter [AWS DMS Task-Logs anzeigen und verwalten](#) im AWS Database Migration Service Benutzerhandbuch.

[DMS.9] DMS-Endpunkte sollten SSL verwenden

Verwandte Anforderungen: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 3, 3, NIST.800-53.r5 SC-2 3 (3), NIST.800-53.r5 SC-2 (4),, NIST.800-53.r5 SC-7 (1), NIST.800-53.r5 SC-8 (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 PCI DSS v4.0.1/4.2.1

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: `AWS::DMS::Endpoint`

AWS Config -Regel: [dms-endpoint-ssl-configured](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein AWS DMS Endpunkt eine SSL-Verbindung verwendet. Die Steuerung schlägt fehl, wenn der Endpunkt kein SSL verwendet.

SSL/TLS-Verbindungen bieten eine Sicherheitsebene, indem sie Verbindungen zwischen DMS-Replikationsinstanzen und Ihrer Datenbank verschlüsseln. Die Verwendung von Zertifikaten bietet eine zusätzliche Sicherheitsebene, indem überprüft wird, ob die Verbindung zur erwarteten Datenbank hergestellt wird. Dazu wird das Serverzertifikat überprüft, das automatisch auf allen von Ihnen bereitgestellten Datenbankinstanzen installiert wird. Indem Sie die SSL-Verbindung auf Ihren DMS-Endpunkten aktivieren, schützen Sie die Vertraulichkeit der Daten während der Migration.

Abhilfe

Informationen zum Hinzufügen einer SSL-Verbindung zu einem neuen oder vorhandenen DMS-Endpunkt finden Sie unter [SSL verwenden mit AWS Database Migration Service](#) im AWS Database Migration Service Benutzerhandbuch.

[DMS.10] Bei DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2,,, 7,, PCI DSS NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6 v4.0.1/7.3.1 NIST.800-53.r5 AC-1 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-5

Kategorie: Schützen > Sichere Zugriffsverwaltung > Passwortlose Authentifizierung

Schweregrad: Mittel

Art der Ressource: AWS::DMS::Endpoint

AWS Config -Regel: [dms-neptune-iam-authorization-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein AWS DMS Endpunkt für eine Amazon Neptune Neptune-Datenbank mit IAM-Autorisierung konfiguriert ist. Die Kontrolle schlägt fehl, wenn für den DMS-Endpunkt keine IAM-Autorisierung aktiviert ist.

AWS Identity and Access Management (IAM) bietet eine differenzierte Zugriffskontrolle für alle Bereiche. AWS Mit IAM können Sie festlegen, wer unter welchen Bedingungen auf welche Dienste und Ressourcen zugreifen kann. Mit IAM-Richtlinien verwalten Sie die Berechtigungen für Ihre Mitarbeiter und Systeme, um sicherzustellen, dass die Berechtigungen mit den geringsten Rechten eingehalten werden. Indem Sie die IAM-Autorisierung auf AWS DMS Endpunkten für Neptune-Datenbanken aktivieren, können Sie IAM-Benutzern Autorisierungsprivilegien gewähren, indem Sie eine durch den Parameter angegebene Servicerolle verwenden. ServiceAccessRoleARN

Abhilfe

Informationen zur Aktivierung der IAM-Autorisierung auf DMS-Endpunkten für Neptune-Datenbanken finden Sie unter [Verwenden von Amazon Neptune als](#) Ziel für im Benutzerhandbuch. AWS Database Migration ServiceAWS Database Migration Service

[DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-3,,, PCI DSS NIST.800-53.r5 AC-6 NIST.800-53.r5 IA-2 v4.0.1/7.3.1 NIST.800-53.r5 IA-5

Kategorie: Schützen > Sichere Zugriffsverwaltung > Passwortlose Authentifizierung

Schweregrad: Mittel

Art der Ressource: AWS::DMS::Endpoint

AWS Config -Regel: [dms-mongo-db-authentication-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein AWS DMS Endpunkt für MongoDB mit einem Authentifizierungsmechanismus konfiguriert ist. Die Steuerung schlägt fehl, wenn kein Authentifizierungstyp für den Endpunkt festgelegt ist.

AWS Database Migration Service unterstützt zwei Authentifizierungsmethoden für MongoDB — MONGODB-CR für MongoDB Version 2.x und SCRAM-SHA-1 für MongoDB Version 3.x oder höher. Diese Authentifizierungsmethoden werden verwendet, um MongoDB-Passwörter zu authentifizieren und zu verschlüsseln, wenn Benutzer die Passwörter für den Zugriff auf die Datenbanken verwenden möchten. Durch die Authentifizierung auf AWS DMS Endpunkten wird sichergestellt, dass nur autorisierte Benutzer auf die Daten zugreifen und diese ändern können, die zwischen Datenbanken migriert werden. Ohne ordnungsgemäße Authentifizierung können unbefugte Benutzer während des Migrationsprozesses möglicherweise auf sensible Daten zugreifen. Dies kann zu Datenschutzverletzungen, Datenverlust oder anderen Sicherheitsvorfällen führen.

Abhilfe

Informationen zur Aktivierung eines Authentifizierungsmechanismus auf DMS-Endpunkten für MongoDB finden Sie unter [Verwenden von MongoDB als Quelle für AWS DMS im Benutzerhandbuch](#).AWS Database Migration Service

[DMS.12] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein

Verwandte Anforderungen:, 3, PCI DSS NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-1 v4.0.1/4.2.1

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: AWS::DMS::Endpoint

AWS Config -Regel: [dms-redis-tls-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein AWS DMS Endpunkt für Redis OSS mit einer TLS-Verbindung konfiguriert ist. Die Steuerung schlägt fehl, wenn auf dem Endpunkt TLS nicht aktiviert ist.

TLS bietet end-to-end Sicherheit, wenn Daten zwischen Anwendungen oder Datenbanken über das Internet gesendet werden. Wenn Sie die SSL-Verschlüsselung für Ihren DMS-Endpunkt konfigurieren, ermöglicht sie die verschlüsselte Kommunikation zwischen der Quell- und der Zieldatenbank während des Migrationsprozesses. Dies trägt dazu bei, das Abhören und Abfangen sensibler Daten durch böswillige Akteure zu verhindern. Ohne SSL-Verschlüsselung kann auf sensible Daten zugegriffen werden, was zu Datenschutzverletzungen, Datenverlust oder anderen Sicherheitsvorfällen führen kann.

Abhilfe

Informationen zum Aktivieren einer TLS-Verbindung auf DMS-Endpunkten für Redis finden Sie unter [Verwenden von Redis als Ziel für AWS Database Migration Service](#) im Benutzerhandbuch.AWS Database Migration Service

Security Hub-Steuerelemente für Amazon DocumentDB

Diese AWS Security Hub Kontrollen bewerten den Service und die Ressourcen von Amazon DocumentDB (mit MongoDB-Kompatibilität). Die Steuerelemente sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 (1), (10), NIST.800-53.R5 NIST.800-53.r5 SC-2 SI-7 NIST.800-53.r5 SC-7 (6)

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: AWS::RDS::DBCluster

AWS Config -Regel: [docdb-cluster-encrypted](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon DocumentDB-Cluster im Ruhezustand verschlüsselt ist. Die Kontrolle schlägt fehl, wenn ein Amazon DocumentDB-Cluster im Ruhezustand nicht verschlüsselt ist.

Daten im Ruhezustand beziehen sich auf alle Daten, die für einen beliebigen Zeitraum in einem persistenten, nichtflüchtigen Speicher gespeichert werden. Durch Verschlüsselung können Sie die Vertraulichkeit solcher Daten schützen und so das Risiko verringern, dass ein nicht autorisierter Benutzer darauf zugreifen kann. Daten in Amazon DocumentDB-Clustern sollten im Ruhezustand verschlüsselt werden, um eine zusätzliche Sicherheitsebene zu gewährleisten. Amazon DocumentDB verwendet den 256-Bit-Advanced Encryption Standard (AES-256), um Ihre Daten mit den in () gespeicherten Verschlüsselungsschlüsseln zu verschlüsseln. AWS Key Management Service AWS KMS

Abhilfe

Sie können die Verschlüsselung im Ruhezustand aktivieren, wenn Sie einen Amazon DocumentDB-Cluster erstellen. Sie können die Verschlüsselungseinstellungen nach dem Erstellen eines Clusters nicht ändern. Weitere Informationen finden Sie unter [Enabling at rest encryption for a Amazon DocumentDB cluster](#) im Amazon DocumentDB Developer Guide.

[DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen

Verwandte Anforderungen: NIST.800-53.R5 SI-12, PCI DSS v4.0.1/3.2.1

Kategorie: Wiederherstellung > Ausfallsicherheit > Backups aktiviert

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: [docdb-cluster-backup-retention-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Standardwert	
<code>minimumBackupRetentionPeriod</code>	Minimale Aufbewahrungsdauer für Backups in Tagen	Ganzzahl	7 auf 35	7	

Diese Kontrolle prüft, ob ein Amazon DocumentDB-Cluster eine Aufbewahrungsdauer für Backups hat, die größer oder gleich dem angegebenen Zeitraum ist. Die Kontrolle schlägt fehl, wenn die Aufbewahrungsfrist für Backups den angegebenen Zeitraum unterschreitet. Sofern Sie keinen benutzerdefinierten Parameterwert für die Aufbewahrungsdauer von Backups angeben, verwendet Security Hub einen Standardwert von 7 Tagen.

Backups helfen Ihnen, sich nach einem Sicherheitsvorfall schneller zu erholen und die Widerstandsfähigkeit Ihrer Systeme zu stärken. Durch die Automatisierung von Backups für Ihre Amazon DocumentDB-Cluster können Sie Ihre Systeme zu einem bestimmten Zeitpunkt wiederherstellen und Ausfallzeiten und Datenverluste minimieren. In Amazon DocumentDB haben Cluster eine standardmäßige Aufbewahrungsfrist für Backups von einem Tag. Dieser Wert muss auf einen Wert zwischen 7 und 35 Tagen erhöht werden, um diese Kontrolle zu bestehen.

Abhilfe

Informationen zum Ändern der Aufbewahrungsdauer von Backups für Ihre Amazon DocumentDB-Cluster finden Sie unter [Ändern eines Amazon DocumentDB-Clusters im Amazon DocumentDB Developer Handbook](#). Wählen Sie für Backup den Aufbewahrungszeitraum für Backups aus.

[DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI NIST.800-53.r5 SC-7 DSS v4.0.1/1.4.4

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Kritisch

Art der Ressource: AWS::RDS::DBClusterSnapshot

AWS Config -Regel: [docdb-cluster-snapshot-public-prohibited](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein manueller Amazon DocumentDB-Cluster-Snapshot öffentlich ist. Die Kontrolle schlägt fehl, wenn der manuelle Cluster-Snapshot öffentlich ist.

Ein manueller Amazon DocumentDB-Cluster-Snapshot sollte nicht öffentlich sein, es sei denn, dies ist beabsichtigt. Wenn Sie einen unverschlüsselten manuellen Snapshot als öffentlich freigeben, ist der Snapshot für alle verfügbar. AWS-Konten Öffentliche Snapshots können zu einer unbeabsichtigten Offenlegung von Daten führen.

Note

Dieses Steuerelement wertet manuelle Cluster-Snapshots aus. Sie können keinen automatisierten Amazon DocumentDB-Cluster-Snapshot teilen. Sie können jedoch einen manuellen Snapshot erstellen, indem Sie den automatisierten Snapshot kopieren und die Kopie dann teilen.

Abhilfe

Informationen zum Entfernen des öffentlichen Zugriffs für manuelle Cluster-Snapshots von Amazon DocumentDB finden Sie unter [Einen Snapshot teilen](#) im Amazon DocumentDB DocumentDB-

Entwicklerhandbuch. Programmgesteuert können Sie den Amazon DocumentDB DocumentDB-Vorgang verwenden. `modify-db-snapshot-attribute` Stellen Sie `attribute-name` als und als ein. `restore values-to-remove all`

[DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), (9), NIST.800-53.r5 AC-6 NIST.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8), PCI DSS v4.0.1/10.3.3

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Ressourcentyp: AWS::RDS::DBCluster

AWS Config -Regel: [docdb-cluster-audit-logging-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon DocumentDB-Cluster Audit-Logs in Amazon CloudWatch Logs veröffentlicht. Die Kontrolle schlägt fehl, wenn der Cluster keine Audit-Logs in Logs veröffentlicht. CloudWatch

Amazon DocumentDB (mit MongoDB-Kompatibilität) ermöglicht es Ihnen, Ereignisse zu überprüfen, die in Ihrem Cluster durchgeführt wurden. Beispiele für protokollierte Ereignisse sind erfolgreiche und fehlgeschlagene Authentifizierungsversuche, Drop-Ereignisse für Sammlungen in einer Datenbank oder das Erstellen eines Index. Standardmäßig ist die Prüfung in Amazon DocumentDB deaktiviert und erfordert, dass Sie Maßnahmen ergreifen, um sie zu aktivieren.

Abhilfe

Informationen zum Veröffentlichen von Amazon DocumentDB-Prüfprotokollen in CloudWatch Logs finden Sie unter [Enabling Auditing](#) im Amazon DocumentDB Developer Guide.

[DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), (2) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5

Kategorie: Schützen > Datenschutz > Schutz vor Datenlöschung

Schweregrad: Mittel

Art der Ressource: AWS::RDS::DBCluster

AWS Config -Regel: [docdb-cluster-deletion-protection-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob in einem Amazon DocumentDB-Cluster der Löschschutz aktiviert ist. Die Kontrolle schlägt fehl, wenn für den Cluster kein Löschschutz aktiviert ist.

Die Aktivierung des Cluster-Löschschutzes bietet einen zusätzlichen Schutz vor versehentlichem Löschen von Datenbanken oder vor dem Löschen durch einen nicht autorisierten Benutzer. Ein Amazon DocumentDB-Cluster kann nicht gelöscht werden, solange der Löschschutz aktiviert ist. Sie müssen zuerst den Löschschutz deaktivieren, bevor eine Löschanfrage erfolgreich sein kann. Der Löschschutz ist standardmäßig aktiviert, wenn Sie einen Cluster in der Amazon DocumentDB DocumentDB-Konsole erstellen.

Abhilfe

Informationen zum Aktivieren des Löschschutzes für einen vorhandenen Amazon DocumentDB-Cluster finden Sie unter [Ändern eines Amazon DocumentDB-Clusters im Amazon DocumentDB DocumentDB-Entwicklerhandbuch](#). Wählen Sie im Abschnitt „Cluster modifizieren“ die Option „Für den Löschschutz aktivieren“.

[DocumentDB.6] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: AWS::RDS::DBCluster

AWS Config -Regel: [docdb-cluster-encrypted-in-transit](#)

Art des Zeitplans: Periodisch

Parameter **excludeTlsParameters**: disabled, enabled (nicht anpassbar)

Diese Steuerung prüft, ob ein Amazon DocumentDB-Cluster TLS für Verbindungen zum Cluster benötigt. Die Steuerung schlägt fehl, wenn die dem Cluster zugeordnete Cluster-Parametergruppe nicht synchronisiert ist oder der TLS-Cluster-Parameter auf disabled oder enabled gesetzt ist.

Sie können TLS verwenden, um die Verbindung zwischen einer Anwendung und einem Amazon DocumentDB-Cluster zu verschlüsseln. Die Verwendung von TLS kann dazu beitragen, Daten davor zu schützen, dass sie abgefangen werden, während die Daten zwischen einer Anwendung und einem Amazon DocumentDB-Cluster übertragen werden. Die Verschlüsselung während der Übertragung für einen Amazon DocumentDB-Cluster wird mithilfe des TLS-Parameters in der Cluster-Parametergruppe verwaltet, die dem Cluster zugeordnet ist. Wenn die Verschlüsselung während der Übertragung aktiviert ist, sind sichere Verbindungen mit TLS erforderlich, um eine Verbindung mit dem Cluster herzustellen. Wir empfehlen die Verwendung der folgenden TLS-Parameter: `tls1.2+tls1.3+`, und `fips-140-3`.

Abhilfe

Informationen zum Ändern der TLS-Einstellungen für einen Amazon DocumentDB-Cluster finden Sie unter [Verschlüsseln von Daten bei der Übertragung im](#) Amazon DocumentDB Developer Guide.

Security Hub-Steuerelemente für DynamoDB

Diese AWS Security Hub Kontrollen bewerten den Service und die Ressourcen von Amazon DynamoDB. Die Steuerelemente sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[DynamoDB.1] DynamoDB-Tabellen sollten die Kapazität automatisch bei Bedarf skalieren

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2(2), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: AWS::DynamoDB::Table

AWS Config -Regel: [dynamodb-autoscaling-enabled](#)

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Gültige benutzerdefinierte Werte	Security Hub Hub-Standardwert
minProvisionedReadCapacity	Mindestanzahl bereitgestellter Lesekapazitätseinheiten für DynamoDB Auto Scaling	Ganzzahl	1 auf 40000	Kein Standardwert
targetReadUtilization	Zielauslastung in Prozent für die Lesekapazität	Ganzzahl	20 auf 90	Kein Standardwert
minProvisionedWriteCapacity	Mindestanzahl bereitgestellter Schreibkapazitätseinheiten für DynamoDB Auto Scaling	Ganzzahl	1 auf 40000	Kein Standardwert
targetWriteUtilization	Zielauslastung in Prozent für die Schreibkapazität	Ganzzahl	20 auf 90	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon DynamoDB-Tabelle ihre Lese- und Schreibkapazität nach Bedarf skalieren kann. Die Steuerung schlägt fehl, wenn die Tabelle nicht den On-Demand-Kapazitätsmodus oder den Bereitstellungsmodus mit konfigurierter Autoskalierung verwendet. Standardmäßig erfordert dieses Steuerelement nur, dass einer dieser Modi konfiguriert

ist, unabhängig von bestimmten Lese- oder Schreibkapazitätsstufen. Optional können Sie benutzerdefinierte Parameterwerte angeben, um bestimmte Lese- und Schreibkapazitäten oder eine bestimmte Zielauslastung zu erfordern.

Durch die bedarfsgerechte Skalierung der Kapazität werden Drosselungen von Ausnahmen vermieden, wodurch die Verfügbarkeit Ihrer Anwendungen aufrechterhalten wird. DynamoDB-Tabellen, die den On-Demand-Kapazitätsmodus verwenden, sind nur durch die standardmäßigen Tabellenkontingente für den DynamoDB-Durchsatz begrenzt. Um diese Kontingente zu erhöhen, können Sie ein Supportticket bei einreichen. Support DynamoDB-Tabellen, die den Bereitstellungsmodus mit Auto Scaling verwenden, passen die bereitgestellte Durchsatzkapazität dynamisch an Verkehrsmuster an. Weitere Informationen zur DynamoDB-Anforderungsdrosselung finden Sie unter Anforderungsdrosselung [und Burstkapazität im Amazon](#) DynamoDB DynamoDB-Entwicklerhandbuch.

Abhilfe

Informationen zur Aktivierung der automatischen DynamoDB-Skalierung für bestehende Tabellen im Kapazitätsmodus finden Sie unter [Aktivieren der auto Skalierung von DynamoDB für bestehende Tabellen](#) im Amazon DynamoDB DynamoDB-Entwicklerhandbuch.

[DynamoDB.2] Bei DynamoDB-Tabellen sollte die Wiederherstellung aktiviert sein point-in-time

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-12, NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Backups aktiviert

Schweregrad: Mittel

Ressourcentyp: AWS::DynamoDB::Table

AWS Config -Regel: [dynamodb-pitr-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob point-in-time Recovery (PITR) für eine Amazon DynamoDB-Tabelle aktiviert ist.

Mithilfe von Backups können Sie sich nach einem Sicherheitsvorfall schneller erholen. Sie stärken auch die Widerstandsfähigkeit Ihrer Systeme. Die point-in-time DynamoDB-Wiederherstellung automatisiert Backups für DynamoDB-Tabellen. Es reduziert die Zeit für die Wiederherstellung nach versehentlichen Lösch- oder Schreibvorgängen. DynamoDB-Tabellen, für die PITR aktiviert ist, können zu einem beliebigen Zeitpunkt der letzten 35 Tage wiederhergestellt werden.

Abhilfe

Informationen zum Wiederherstellen einer DynamoDB-Tabelle auf einen bestimmten Zeitpunkt finden Sie unter [Wiederherstellen einer DynamoDB-Tabelle auf einen bestimmten Zeitpunkt im Amazon DynamoDB](#) DynamoDB-Entwicklerhandbuch.

[DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 (1), (10), NIST.800-53.R5 NIST.800-53.r5 SC-2 SI-7 NIST.800-53.r5 SC-7 (6)

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: AWS::DAX::Cluster

AWS Config -Regel: [dax-encryption-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon DynamoDB Accelerator (DAX) -Cluster im Ruhezustand verschlüsselt ist. Die Steuerung schlägt fehl, wenn der DAX-Cluster im Ruhezustand nicht verschlüsselt ist.

Durch die Verschlüsselung von Daten im Ruhezustand wird das Risiko verringert, dass auf Daten, die auf der Festplatte gespeichert sind, von einem Benutzer zugegriffen wird, für den keine Authentifizierung angemeldet ist. AWS Durch die Verschlüsselung werden weitere Zugriffskontrollen hinzugefügt, um den Zugriff nicht autorisierter Benutzer auf die Daten zu beschränken. Beispielsweise sind API-Berechtigungen erforderlich, um die Daten zu entschlüsseln, bevor sie gelesen werden können.

Abhilfe

Sie können die Verschlüsselung im Ruhezustand nicht aktivieren oder deaktivieren, nachdem ein Cluster erstellt wurde. Sie müssen den Cluster neu erstellen, um die Verschlüsselung im Ruhezustand zu aktivieren. Ausführliche Anweisungen zum Erstellen eines DAX-Clusters mit aktivierter Verschlüsselung im Ruhezustand finden Sie unter [Enabling at rest using the AWS Management Console](#) im Amazon DynamoDB Developer Guide.

[DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-12, NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Backups aktiviert

Schweregrad: Mittel

Ressourcentyp: AWS::DynamoDB::Table

AWS Config Regel: [dynamodb-resources-protected-by-backup-plan](#)

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
backupVaultLockCheck	Das Steuerelement ermittelt, ob der Parameter auf <code>true</code> gesetzt ist und die Ressource AWS Backup Vault Lock verwendet.	Boolesch	<code>true</code> oder <code>false</code>	Kein Standardwert

Dieses Steuerelement bewertet, ob eine Amazon DynamoDB-Tabelle im ACTIVE Status durch einen Backup-Plan abgedeckt ist. Die Steuerung schlägt fehl, wenn die DynamoDB-Tabelle nicht durch einen Backup-Plan abgedeckt ist. Wenn Sie den `backupVaultLockCheck` Parameter auf gleich

setzen `true`, wird die Steuerung nur erfolgreich, wenn die DynamoDB-Tabelle in einem AWS Backup gesicherten Tresor gesichert ist.

AWS Backup ist ein vollständig verwalteter Backup-Service, der Ihnen hilft, die Sicherung von Daten auf allen Ebenen zu zentralisieren und zu automatisieren. AWS-Services Mit AWS Backup können Sie Backup-Pläne erstellen, die Ihre Backup-Anforderungen definieren, z. B. wie oft Ihre Daten gesichert werden sollen und wie lange diese Backups aufbewahrt werden sollen. Wenn Sie DynamoDB-Tabellen in Ihre Backup-Pläne aufnehmen, können Sie Ihre Daten vor unbeabsichtigtem Verlust oder Löschung schützen.

Abhilfe

Informationen zum Hinzufügen einer DynamoDB-Tabelle zu einem AWS Backup Backup-Plan finden Sie unter [Zuweisen von Ressourcen zu einem Backup-Plan im AWS Backup Entwicklerhandbuch](#).

[DynamoDB.5] DynamoDB-Tabellen sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::DynamoDB::Table`

AWS Config Regel: `tagged-dynamodb-table` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob eine Amazon DynamoDB-Tabelle Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind. `requiredTagKeys` Das Steuerelement schlägt fehl, wenn die Tabelle keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält. `requiredTagKeys` Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Tabelle mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer DynamoDB-Tabelle finden Sie unter [Tagging resources in DynamoDB im Amazon DynamoDB Developer Guide](#).

[DynamoDB.6] Bei DynamoDB-Tabellen sollte der Löschschutz aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), (2) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5

Kategorie: Schützen > Datenschutz > Schutz vor Datenlöschung

Schweregrad: Mittel

Art der Ressource: AWS::DynamoDB::Table

AWS Config Regel: [dynamodb-table-deletion-protection-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für eine Amazon DynamoDB-Tabelle der Löschschutz aktiviert ist. Das Steuerelement schlägt fehl, wenn für eine DynamoDB-Tabelle kein Löschschutz aktiviert ist.

Mit der Eigenschaft Löschschutz können Sie eine DynamoDB-Tabelle vor versehentlichem Löschen schützen. Durch die Aktivierung dieser Eigenschaft für Tabellen wird sichergestellt, dass Tabellen nicht versehentlich während der regulären Tabellenverwaltung durch Ihre Administratoren gelöscht werden. Dies trägt dazu bei, Störungen Ihres normalen Geschäftsbetriebs zu vermeiden.

Abhilfe

Informationen zum Aktivieren des Löschschutzes für eine DynamoDB-Tabelle finden Sie unter [Verwenden des Löschschutzes](#) im Amazon DynamoDB DynamoDB-Entwicklerhandbuch.

[DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 AC-1 7, 3, NIST.800-53.r5 SC-1 3 NIST.800-53.r5 SC-8, PCI DSS v4.0.1/4.2.1 NIST.800-53.r5 SC-2

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: AWS::DAX::Cluster

AWS Config -Regel: [dax-tls-endpoint-encryption](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon DynamoDB Accelerator (DAX) -Cluster während der Übertragung verschlüsselt ist, wobei der Endpunktverschlüsselungstyp auf TLS festgelegt ist. Die Steuerung schlägt fehl, wenn der DAX-Cluster bei der Übertragung nicht verschlüsselt wird.

HTTPS (TLS) kann verwendet werden, um zu verhindern, dass potenzielle Angreifer person-in-the-middle oder ähnliche Angriffe verwenden, um den Netzwerkverkehr zu belauschen oder zu manipulieren. Sie sollten nur verschlüsselte Verbindungen über TLS für den Zugriff auf DAX-Cluster zulassen. Die Verschlüsselung von Daten während der Übertragung kann jedoch die Leistung beeinträchtigen. Sie sollten Ihre Anwendung mit aktivierter Verschlüsselung testen, um das Leistungsprofil und die Auswirkungen von TLS zu verstehen.

Abhilfe

Sie können die TLS-Verschlüsselungseinstellung nicht ändern, nachdem Sie einen DAX-Cluster erstellt haben. Um einen vorhandenen DAX-Cluster zu verschlüsseln, erstellen Sie einen neuen Cluster mit aktivierter Verschlüsselung bei der Übertragung, verlagern Sie den Datenverkehr Ihrer Anwendung darauf und löschen Sie dann den alten Cluster. Weitere Informationen finden Sie unter [Verwenden des Löschschutzes](#) im Amazon DynamoDB DynamoDB-Entwicklerhandbuch.

Security Hub-Steuerelemente für Amazon EC2

Diese AWS Security Hub Kontrollen bewerten den Service und die Ressourcen von Amazon Elastic Compute Cloud (Amazon EC2). Die Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[EC2.1] Amazon EBS-Snapshots sollten nicht öffentlich wiederherstellbar sein

Verwandte Anforderungen: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/7.2.1, NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3, (21), (11) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (16) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Kritisch

Ressourcentyp: AWS:::Account

AWS Config -Regel: [ebs-snapshot-public-restorable-check](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob Amazon Elastic Block Store-Snapshots nicht öffentlich sind. Die Kontrolle schlägt fehl, wenn Amazon EBS-Snapshots von jedermann wiederhergestellt werden können.

EBS-Snapshots werden verwendet, um die Daten auf Ihren EBS-Volumes zu einem bestimmten Zeitpunkt auf Amazon S3 zu sichern. Sie können die Snapshots verwenden, um frühere Status von EBS-Volumes wiederherzustellen. Es ist selten akzeptabel, einen Snapshot mit der Öffentlichkeit zu teilen. Typischerweise wurde die Entscheidung, eine Momentaufnahme öffentlich zu teilen, irrtümlich oder ohne vollständiges Verständnis der Auswirkungen getroffen. Diese Überprüfung trägt dazu bei, dass alle diese Freigaben vollständig geplant und beabsichtigt waren.

Abhilfe

Informationen dazu, wie Sie einen öffentlichen EBS-Snapshot privat machen können, finden [Sie unter Einen Snapshot teilen](#) im EC2 Amazon-Benutzerhandbuch. Wählen Sie für Aktionen, Berechtigungen ändern die Option Privat aus.

[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen

Verwandte Anforderungen: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/2.1, CIS AWS Foundations Benchmark v1.2.0/4.3, CIS Foundations Benchmark v1.4.0/5.3, CIS AWS Foundations Benchmark v3.0.0/5.4,, (21), (11), (16) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (21), (4), NIST.800-53.r5 SC-7 (5) AWS NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Hoch

Art der Ressource: AWS::EC2::SecurityGroup

AWS Config -Regel: [vpc-default-security-group-closed](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Standardsicherheitsgruppe einer VPC eingehenden oder ausgehenden Datenverkehr zulässt. Die Steuerung schlägt fehl, wenn die Sicherheitsgruppe eingehenden oder ausgehenden Datenverkehr zulässt.

Die Regeln für die [Standardsicherheitsgruppe](#) erlauben den gesamten ausgehenden und eingehenden Datenverkehr von Netzwerkschnittstellen (und den zugehörigen Instances), die derselben Sicherheitsgruppe zugewiesen sind. Wir empfehlen, die Standardsicherheitsgruppe nicht zu verwenden. Da die Standardsicherheitsgruppe nicht gelöscht werden kann, sollten Sie die Standardeinstellung für Sicherheitsgruppenregeln ändern, um eingehenden und ausgehenden Datenverkehr einzuschränken. Dadurch wird unbeabsichtigter Datenverkehr verhindert, falls die Standardsicherheitsgruppe versehentlich für Ressourcen wie EC2 Instances konfiguriert wird.

Abhilfe

Um dieses Problem zu beheben, erstellen Sie zunächst neue Sicherheitsgruppen mit den geringsten Rechten. Anweisungen finden Sie unter [Erstellen einer Sicherheitsgruppe](#) im Amazon VPC-Benutzerhandbuch. Weisen Sie dann die neuen Sicherheitsgruppen Ihren EC2 Instances zu. Anweisungen finden Sie unter [Ändern der Sicherheitsgruppe einer Instance](#) im EC2 Amazon-Benutzerhandbuch.

Nachdem Sie Ihren Ressourcen die neuen Sicherheitsgruppen zugewiesen haben, entfernen Sie alle Regeln für eingehenden und ausgehenden Datenverkehr aus den Standardsicherheitsgruppen. Anweisungen finden [Sie unter Sicherheitsgruppenregeln konfigurieren](#) im Amazon VPC-Benutzerhandbuch.

[EC2.3] Angehängte Amazon EBS-Volumes sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), (10), NIST.800-53.R5 SI-7 NIST.800-53.r5 SC-7 (6)

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: AWS::EC2::Volume

AWS Config -Regel: [encrypted-volumes](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die EBS-Volumes, die sich im angefügten Zustand befinden, verschlüsselt sind. Um diese Prüfung zu bestehen, müssen EBS-Volumes in Betrieb und verschlüsselt sein. Wenn das EBS-Volume nicht angefügt ist, unterliegt es nicht dieser Prüfung.

Um eine zusätzliche Sicherheitsebene Ihrer sensiblen Daten in EBS-Volumes zu gewährleisten, sollten Sie die EBS-Verschlüsselung im Ruhezustand aktivieren. Die Amazon EBS-Verschlüsselung bietet eine einfache Verschlüsselungslösung für Ihre EBS-Ressourcen, ohne dass Sie eine eigene Infrastruktur für die Schlüsselverwaltung erstellen, verwalten und sichern müssen. Bei der Erstellung verschlüsselter Volumes und Snapshots werden KMS-Schlüssel verwendet.

Weitere Informationen zur Amazon EBS-Verschlüsselung finden Sie unter [Amazon EBS-Verschlüsselung](#) im EC2 Amazon-Benutzerhandbuch.

Abhilfe

Es gibt keine direkte Möglichkeit, ein vorhandenes unverschlüsseltes Volume oder einen Snapshot zu verschlüsseln. Sie können ein neues Volume oder einen neuen Snapshot nur beim Erstellen verschlüsseln.

Wenn Sie die Verschlüsselung standardmäßig aktiviert haben, verschlüsselt Amazon EBS das resultierende neue Volume oder den Snapshot mit Ihrem Standardschlüssel für die Amazon EBS-Verschlüsselung. Auch wenn Sie die standardmäßige Verschlüsselung nicht aktiviert haben, können Sie die Verschlüsselung beim Erstellen eines einzelnen Volumes oder Snapshots aktivieren. In beiden Fällen können Sie den Standardschlüssel für die Amazon EBS-Verschlüsselung überschreiben und einen symmetrischen, vom Kunden verwalteten Schlüssel wählen.

Weitere Informationen finden Sie unter [Erstellen eines Amazon EBS-Volumes](#) und [Kopieren eines Amazon EBS-Snapshots](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.4] Gestoppte EC2 Instances sollten nach einem bestimmten Zeitraum entfernt werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2)

Kategorie: Identifizieren > Bestand

Schweregrad: Mittel

Art der Ressource: AWS::EC2::Instance

AWS Config -Regel: [ec2-stopped-instance](#)

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
AllowedDays	Anzahl der Tage, an denen sich die EC2 Instance im gestoppten Zustand befinden darf, bevor ein fehlgeschlagenes Ergebnis generiert wird.	Ganzzahl	1 auf 365	30

Diese Kontrolle prüft, ob eine EC2 Amazon-Instance länger als die zulässige Anzahl von Tagen gestoppt wurde. Die Kontrolle schlägt fehl, wenn eine EC2 Instance länger als die maximal zulässige Zeitspanne angehalten wird. Sofern Sie keinen benutzerdefinierten Parameterwert für den maximal zulässigen Zeitraum angeben, verwendet Security Hub einen Standardwert von 30 Tagen.

Wenn eine EC2 Instanz über einen längeren Zeitraum nicht ausgeführt wurde, stellt dies ein Sicherheitsrisiko dar, da die Instanz nicht aktiv gewartet (analysiert, gepatcht, aktualisiert) wird. Wenn sie später gestartet wird, kann der Mangel an ordnungsgemäßer Wartung zu unerwarteten Problemen in Ihrer AWS Umgebung führen. Um eine EC2 Instance über einen längeren Zeitraum sicher inaktiv zu halten, starten Sie sie regelmäßig zu Wartungszwecken und beenden Sie sie dann nach der Wartung. Idealerweise sollte dies ein automatisierter Prozess sein.

Abhilfe

Informationen zum Beenden einer inaktiven EC2 Instance finden Sie unter [Kündigen einer Instance](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.6] Die VPC-Flow-Protokollierung sollte in allen aktiviert sein VPCs

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/2.9, CIS Foundations Benchmark v1.4.0/3.9, CIS AWS Foundations Benchmark v3.0.0/3.7, NIST.800-53.r5 AC-4 (26), NIST.800-53.R5 SI-7 (8), NIST.800-171.r2 3.1.20 NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-171.r2 3.3.1, NIST.800-171.r2 3.13.1, PCI DSS v3.2.1/10.3.3, PCI DSS v3.2.1/10.3.3 2.1/10.3.4, PCI DSS v3.2.1/10.3.5, PCI DSS v3.2.1/10.3.6 AWS

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS::EC2::VPC

AWS Config -Regel: [vpc-flow-logs-enabled](#)

Art des Zeitplans: Periodisch

Parameter:

- `trafficType`: REJECT (nicht anpassbar)

Dieses Steuerelement prüft, ob Amazon VPC Flow Logs gefunden und aktiviert wurden. VPCs Der Verkehrstyp ist auf Reject eingestellt. Die Steuerung schlägt fehl, wenn VPC Flow Logs VPCs in Ihrem Konto nicht aktiviert sind.

Note

Dieses Steuerelement überprüft nicht, ob Amazon VPC Flow Logs über Amazon Security Lake für aktiviert sind. AWS-Konto

Mit der Funktion VPC Flow Logs können Sie Informationen über den IP-Adressverkehr zu und von Netzwerkschnittstellen in Ihrer VPC erfassen. Nachdem Sie ein Flow-Protokoll erstellt haben, können Sie die zugehörigen Daten in CloudWatch Logs anzeigen und abrufen. Um die Kosten zu senken, können Sie Ihre Flow-Logs auch an Amazon S3 senden.

Security Hub empfiehlt, die Flussprotokollierung für zurückgewiesene Pakete für zu aktivieren. VPCs Flow-Logs bieten Einblick in den Netzwerkverkehr, der die VPC durchquert, und können anomalen Datenverkehr erkennen oder Einblicke in Sicherheitsworkflows geben.

Standardmäßig enthält der Datensatz Werte für die verschiedenen Komponenten des IP-Adressflusses, einschließlich Quelle, Ziel und Protokoll. Weitere Informationen und Beschreibungen der Protokollfelder finden Sie unter [VPC Flow Logs](#) im Amazon VPC-Benutzerhandbuch.

Abhilfe

Informationen zum Erstellen eines VPC-Flow-Protokolls finden Sie unter [Erstellen eines Flow-Protokolls](#) im Amazon VPC-Benutzerhandbuch. Nachdem Sie die Amazon VPC-Konsole geöffnet haben, wählen Sie Your VPCs. Wählen Sie für Filter Ablehnen oder Alle.

[EC2.7] Die EBS-Standardverschlüsselung sollte aktiviert sein

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.4.0/2.2.1, CIS AWS Foundations Benchmark v3.0.0/2.2.1, (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 NIST.800-53.r5 CA-9 (1), (10), NIST.800-53.r5 NIST.800-53.r5 SC-2 SI-7 (6) NIST.800-53.r5 SC-7

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: AWS:::Account

AWS Config -Regel: [ec2-ebs-encryption-by-default](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob die Verschlüsselung auf Kontoebene standardmäßig für Amazon Elastic Block Store (Amazon EBS) -Volumes aktiviert ist. Die Kontrolle schlägt fehl, wenn die Verschlüsselung auf Kontoebene für EBS-Volumes nicht aktiviert ist.

Wenn die Verschlüsselung für Ihr Konto aktiviert ist, werden Amazon EBS-Volumes und Snapshot-Kopien im Ruhezustand verschlüsselt. Dies bietet eine zusätzliche Schutzebene für Ihre Daten. Weitere Informationen finden Sie unter [Standardverschlüsselung](#) im EC2 Amazon-Benutzerhandbuch.

Abhilfe

Informationen zur Konfiguration der Standardverschlüsselung für Amazon EBS-Volumes finden Sie [unter Standardverschlüsselung](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.8] EC2 Instances sollten Instance Metadata Service Version 2 () verwenden IMDSv2

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/5.6., NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3, PCI DSS v4.0.1/2.2.6 NIST.800-53.r5 AC-6

Kategorie: Schützen > Netzwerksicherheit

Schweregrad: Hoch

Art der Ressource: AWS::EC2::Instance

AWS Config -Regel: [ec2-imdsv2-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Ihre EC2 Instanz-Metadatenversion mit Version 2 (IMDSv2) für den Instanz-Metadatendienst konfiguriert ist. Das Steuerelement `HttpTokens` ist erfolgreich, wenn es auf erforderlich für gesetzt ist IMDSv2. Das Steuerelement schlägt fehl, wenn auf gesetzt `HttpTokens` ist `optional`.

Sie verwenden Instanz-Metadaten, um die laufende Instanz zu konfigurieren oder zu verwalten. Das IMDS bietet Zugriff auf temporäre, häufig wechselnde Anmeldeinformationen. Mit diesen Anmeldeinformationen entfällt die Notwendigkeit, vertrauliche Anmeldeinformationen manuell oder programmgesteuert fest zu codieren oder vertrauliche Anmeldeinformationen an Instanzen zu verteilen. Das IMDS ist lokal an jede Instanz angehängt. EC2 Es läuft auf einer speziellen „Link Local“-IP-Adresse 169.254.169.254. Auf diese IP-Adresse kann nur mit Software zugegriffen werden, die auf der Instance ausgeführt wird.

Version 2 des IMDS bietet neue Schutzmaßnahmen für die folgenden Arten von Sicherheitslücken. Diese Sicherheitslücken könnten genutzt werden, um zu versuchen, auf das IMDS zuzugreifen.

- Öffnen Sie die Firewalls für Websites und Anwendungen.
- Öffnen Sie Reverse-Proxys
- Sicherheitslücken bei serverseitiger Anforderungsfälschung (SSRF)
- Offene Layer-3-Firewalls und Network Address Translation (NAT)

Security Hub empfiehlt, dass Sie Ihre EC2 Instanzen mit konfigurieren IMDSv2.

Abhilfe

Informationen zur Konfiguration von EC2 Instances mit IMDSv2 finden Sie unter [Empfohlener Pfad zur Anforderung IMDSv2](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.9] EC2 Amazon-Instances sollten keine öffentliche IPv4 Adresse haben

Verwandte Anforderungen: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Hoch

Art der Ressource: AWS::EC2::Instance

AWS Config -Regel: [ec2-instance-no-public-ip](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob EC2 Instances eine öffentliche IP-Adresse haben. Die Steuerung schlägt fehl, wenn das `publicIp` Feld im EC2 Instanzkonfigurationselement vorhanden ist. Dieses Steuerelement gilt nur für IPv4 Adressen.

Eine öffentliche IPv4 Adresse ist eine IP-Adresse, die über das Internet erreichbar ist. Wenn Sie Ihre Instance mit einer öffentlichen IP-Adresse starten, ist Ihre EC2 Instance über das Internet erreichbar. Eine private IPv4 Adresse ist eine IP-Adresse, die über das Internet nicht erreichbar ist. Sie können private IPv4 Adressen für die Kommunikation zwischen EC2 Instances in derselben VPC oder in Ihrem verbundenen privaten Netzwerk verwenden.

IPv6 Adressen sind weltweit einzigartig und daher über das Internet erreichbar. Standardmäßig ist das IPv6 Adressierungsattribut jedoch in allen Subnetzen auf False gesetzt. Weitere Informationen IPv6 finden Sie unter [IP-Adressierung in Ihrer VPC](#) im Amazon VPC-Benutzerhandbuch.

Wenn Sie einen legitimen Anwendungsfall für die Verwaltung von EC2 Instances mit öffentlichen IP-Adressen haben, können Sie die Ergebnisse dieser Kontrolle unterdrücken. Weitere Informationen zu

Frontend-Architekturoptionen finden Sie im [AWS Architektur-Blog](#) oder in der [AWS Videoserie This Is My Architecture-Serie](#).

Abhilfe

Verwenden Sie eine nicht standardmäßige VPC, damit Ihrer Instance standardmäßig keine öffentliche IP-Adresse zugewiesen wird.

Wenn Sie eine EC2 Instance in einer Standard-VPC starten, wird ihr eine öffentliche IP-Adresse zugewiesen. Wenn Sie eine EC2 Instance in einer nicht standardmäßigen VPC starten, bestimmt die Subnetzkonfiguration, ob sie eine öffentliche IP-Adresse erhält. Das Subnetz verfügt über ein Attribut, das bestimmt, ob neue EC2 Instances im Subnetz eine öffentliche IP-Adresse aus dem öffentlichen Adresspool erhalten. IPv4

Sie können eine automatisch zugewiesene öffentliche IP-Adresse von Ihrer Instance trennen. EC2 Weitere Informationen finden Sie unter [Öffentliche IPv4 Adressen und externe DNS-Hostnamen](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.10] Amazon EC2 sollte so konfiguriert sein, dass es VPC-Endpunkte verwendet, die für den Amazon-Service erstellt wurden EC2

Verwandte Anforderungen: NIST.800-53.r5 AC-2 1,, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3, (21), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (11), (16) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), (3), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.13.1 NIST.800-53.r5 SC-7

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Privater API-Zugriff

Schweregrad: Mittel

Art der Ressource: AWS::EC2::VPC

AWS Config -Regel: [service-vpc-endpoint-enabled](#)

Art des Zeitplans: Periodisch

Parameter:

- `serviceName: ec2` (nicht anpassbar)

Dieses Steuerelement prüft, ob für jede VPC ein Service-Endpunkt für Amazon erstellt EC2 wird. Die Steuerung schlägt fehl, wenn für eine VPC kein VPC-Endpunkt für den EC2 Amazon-Service erstellt wurde.

Diese Kontrolle bewertet Ressourcen in einem einzigen Konto. Es kann keine Ressourcen beschreiben, die sich außerhalb des Kontos befinden. Da AWS Config Security Hub keine kontoübergreifenden Prüfungen durchführt, werden Sie feststellen, VPCs dass die FAILED Ergebnisse für alle Konten gemeinsam genutzt werden. Security Hub empfiehlt, diese FAILED Ergebnisse zu unterdrücken.

Um die Sicherheitslage Ihrer VPC zu verbessern, können Sie Amazon so konfigurieren, EC2 dass es einen VPC-Endpunkt mit Schnittstelle verwendet. Schnittstellenendpunkte werden von einer Technologie unterstützt AWS PrivateLink, mit der Sie privat auf EC2 Amazon-API-Operationen zugreifen können. Es schränkt den gesamten Netzwerkverkehr zwischen Ihrer VPC und Amazon EC2 auf das Amazon-Netzwerk ein. Da Endpoints nur in derselben Region unterstützt werden, können Sie keinen Endpunkt zwischen einer VPC und einem Service in einer anderen Region erstellen. Dies verhindert unbeabsichtigte EC2 Amazon-API-Aufrufe in andere Regionen.

Weitere Informationen zum Erstellen von VPC-Endpunkten für Amazon finden Sie unter [Amazon EC2 EC2 und Interface-VPC-Endpoints](#) im Amazon-Benutzerhandbuch. EC2

Abhilfe

Informationen zum Erstellen eines Schnittstellenendpunkts zu Amazon EC2 von der Amazon VPC-Konsole aus finden Sie unter [Erstellen eines VPC-Endpunkts](#) im AWS PrivateLink Handbuch. Wählen Sie für den Servicenamen com.amazonaws aus. **region**.ec2.

Sie können auch eine Endpunktrichtlinie erstellen und an Ihren VPC-Endpunkt anhängen, um den Zugriff auf die EC2 Amazon-API zu kontrollieren. Anweisungen zur Erstellung einer VPC-Endpunktrichtlinie finden Sie unter [Erstellen einer Endpunktrichtlinie](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.12] Unbenutztes Amazon EC2 EIPs sollte entfernt werden

Verwandte Anforderungen: PCI DSS v3.2.1/2.4, NIST.800-53.R5 CM-8 (1)

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Niedrig

Art der Ressource: AWS::EC2::EIP

AWS Config -Regel: [eip-attached](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Elastic IP (EIP) -Adressen, die einer VPC zugewiesen sind, mit EC2 Instances oder verwendeten Elastic Network Interfaces () verknüpft sind. ENIs

Ein fehlgeschlagenes Ergebnis deutet darauf hin, dass Sie möglicherweise ungenutzte Daten verwendet haben. EC2 EIPs

Auf diese Weise können Sie einen genauen Bestand an Beständen EIPs in Ihrer Karteninhaberdatenumgebung (CDE) verwalten.

Abhilfe

Informationen zur Freigabe einer ungenutzten EIP finden Sie unter [Elastic IP Address veröffentlichen](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.13] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/4.1,, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-4, (11) NIST.800-53.r5 CM-7, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), NIST.800-53.r5 SC-7 NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.13.1, PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/2.2.2, PCI DSS v4.0.1/1.3.1 1.3.1

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Hoch

Art der Ressource: AWS::EC2::SecurityGroup

AWS Config -Regel: [restricted-ssh](#)

Art des Zeitplans: Ausgelöste und periodische Änderung

Parameter: Keine

Diese Kontrolle prüft, ob eine EC2 Amazon-Sicherheitsgruppe den Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulässt. Die Kontrolle schlägt fehl, wenn die Sicherheitsgruppe den Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulässt.

Sicherheitsgruppen bieten eine zustandsorientierte Filterung von ein- und ausgehendem Netzwerkdatenverkehr von bzw. an AWS -Ressourcen. Unsere Empfehlung ist, dass keine Sicherheitsgruppe uneingeschränkten Zugriff auf Port 22 für eingehenden Datenverkehr erlauben sollte. Durch die Unterbindung der uneingeschränkten Konnektivität mit Remote-Konsolenservices wie SSH wird die Risikoaussetzung eines Servers reduziert.

Abhilfe

Um den Zugang zu Port 22 zu verhindern, entfernen Sie die Regel, die diesen Zugriff für jede Sicherheitsgruppe, die einer VPC zugeordnet ist, erlaubt. Anweisungen finden Sie unter [Sicherheitsgruppenregeln aktualisieren](#) im EC2 Amazon-Benutzerhandbuch. Nachdem Sie in der EC2 Amazon-Konsole eine Sicherheitsgruppe ausgewählt haben, wählen Sie Aktionen, Regeln für eingehenden Datenverkehr bearbeiten. Entfernen Sie die Regel, die den Zugriff auf Port 22 ermöglicht.

[EC2.14] Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 oder: :/0 auf Port 3389 zulassen

Verwandte Anforderungen: CIS Foundations Benchmark v1.2.0/4.2, PCI DSS v4.0.1/1.3.1 AWS

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Hoch

Art der Ressource: AWS::EC2::SecurityGroup

AWS Config Regel: [restricted-common-ports](#)(Die erstellte Regel istrestricted-rdp)

Art des Zeitplans: Ausgelöste und periodische Änderung

Parameter: Keine

Diese Kontrolle prüft, ob eine EC2 Amazon-Sicherheitsgruppe den Zugang von 0.0.0.0/0 oder: :/0 zu Port 3389 zulässt. Die Kontrolle schlägt fehl, wenn die Sicherheitsgruppe den Zugriff von 0.0.0.0/0 oder: :/0 auf Port 3389 zulässt.

Sicherheitsgruppen bieten eine zustandsorientierte Filterung von ein- und ausgehendem Netzwerkdatenverkehr von bzw. an AWS -Ressourcen. Unsere Empfehlung ist, dass keine

Sicherheitsgruppe uneingeschränkter Zugriff auf Port 3389 für eingehenden Datenverkehr erlauben sollte. Durch die Unterbindung der uneingeschränkten Konnektivität mit Remote-Konsolenservices wie RDP wird die Risikoaussetzung eines Servers reduziert.

Abhilfe

Um den Zugriff auf Port 3389 zu verhindern, entfernen Sie die Regel, die diesen Zugriff für jede Sicherheitsgruppe, die einer VPC zugeordnet ist, erlaubt. Anweisungen finden Sie unter [Sicherheitsgruppenregeln aktualisieren](#) im Amazon VPC-Benutzerhandbuch. Nachdem Sie in der Amazon VPC-Konsole eine Sicherheitsgruppe ausgewählt haben, wählen Sie Aktionen, Regeln für eingehenden Datenverkehr bearbeiten. Entfernen Sie die Regel, die den Zugriff auf Port 3389 ermöglicht.

[EC2.15] EC2 Amazon-Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen

Verwandte Anforderungen: NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v4.0.1/1.4.4

Kategorie: Schützen > Netzwerksicherheit

Schweregrad: Mittel

Art der Ressource: AWS::EC2::Subnet

AWS Config -Regel: [subnet-auto-assign-public-ip-disabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Zuweisung von öffentlichen Subnetzen IPs in Amazon Virtual Private Cloud (Amazon VPC) auf MapPublicIpOnLaunch eingestellt ist. FALSE Die Kontrolle ist erfolgreich, wenn das Flag auf gesetzt ist. FALSE

Alle Subnetze haben ein Attribut, das bestimmt, ob eine im Subnetz erstellte Netzwerkschnittstelle automatisch eine öffentliche IPv4 Adresse erhält. Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Abhilfe

Informationen zur Konfiguration eines Subnetzes, sodass keine öffentlichen IP-Adressen zugewiesen werden, finden Sie unter [Ändern des öffentlichen IPv4 Adressierungsattributs für Ihr Subnetz](#) im Amazon VPC-Benutzerhandbuch. Deaktivieren Sie das Kontrollkästchen Automatische Zuweisung von öffentlichen IPv4 Adressen aktivieren.

[EC2.16] Ungenutzte Network Access Control Lists sollten entfernt werden

Verwandte Anforderungen: NIST.800-53.R5 CM-8 (1), NIST.800-171.R2 3.4.7, PCI DSS v4.0.1/1.2.7

Kategorie: Schützen > Netzwerksicherheit

Schweregrad: Niedrig

Art der Ressource: AWS::EC2::NetworkACL

AWS Config -Regel: [vpc-network-acl-unused-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob es in Ihrer Virtual Private Cloud (VPC ACLs) ungenutzte Netzwerkzugriffskontrolllisten (Netzwerk) gibt. Die Steuerung schlägt fehl, wenn die Netzwerk-ACL keinem Subnetz zugeordnet ist. Das Steuerelement generiert keine Ergebnisse für eine ungenutzte Standard-Netzwerk-ACL.

Das Steuerelement überprüft die Elementkonfiguration der Ressource AWS::EC2::NetworkACL und bestimmt die Beziehungen der Netzwerk-ACL.

Wenn die einzige Beziehung die VPC der Netzwerk-ACL ist, schlägt die Steuerung fehl.

Wenn andere Beziehungen aufgeführt sind, ist die Kontrolle erfolgreich.

Abhilfe

Anweisungen zum Löschen einer ungenutzten Netzwerk-ACL finden Sie unter [Löschen einer Netzwerk-ACL](#) im Amazon VPC-Benutzerhandbuch. Sie können die Standard-Netzwerk-ACL oder eine ACL, die Subnetzen zugeordnet ist, nicht löschen.

[EC2.17] EC2 Amazon-Instances sollten nicht mehrere verwenden ENIs

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (21)

Kategorie: Schützen > Netzwerksicherheit

Schweregrad: Niedrig

Art der Ressource: AWS::EC2::Instance

AWS Config -Regel: [ec2-instance-multiple-eni-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine EC2 Instance mehrere Elastic Network Interfaces (ENIs) oder Elastic Fabric Adapter (EFAs) verwendet. Dieses Steuerelement ist erfolgreich, wenn ein einziger Netzwerkadapter verwendet wird. Das Steuerelement enthält eine optionale Parameterliste zur Identifizierung der zulässigen Parameter ENIs. Diese Kontrolle schlägt auch fehl, wenn eine EC2 Instance, die zu einem Amazon EKS-Cluster gehört, mehr als eine ENI verwendet. Wenn Ihre EC2 Instances mehrere ENIs als Teil eines Amazon EKS-Clusters benötigen, können Sie diese Kontrollergebnisse unterdrücken.

Mehrere ENIs können zu doppelt vernetzten Instances führen, d. h. zu Instances mit mehreren Subnetzen. Dies kann die Komplexität der Netzwerksicherheit erhöhen und unbeabsichtigte Netzwerkpfade und Zugriffe zur Folge haben.

Abhilfe

Informationen zum Trennen einer Netzwerkschnittstelle von einer EC2 Instance finden Sie unter [Trennen einer Netzwerkschnittstelle von einer Instance](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.18] Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Datenverkehr für autorisierte Ports zulassen

Verwandte Anforderungen: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), (11), (16) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (5), NIST.800-53.r5 SC-7 NIST.800-171.R2 3.1.3, NIST.800-53.r5 SC-7 NIST.800-171.R2 3.1.20, NIST.800-171.R2 3.13.1

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Konfiguration der Sicherheitsgruppe

Schweregrad: Hoch

Art der Ressource: AWS::EC2::SecurityGroup

AWS Config -Regel: [vpc-sg-open-only-to-authorized-ports](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>authorizeTcpPorts</code>	Liste der autorisierten TCP-Ports	IntegerList (mindestens 1 Artikel und maximal 32 Artikel)	1 auf 65535	[80, 443]
<code>authorizeUdpPorts</code>	Liste der autorisierten UDP-Ports	IntegerList (mindestens 1 Artikel und maximal 32 Artikel)	1 auf 65535	Kein Standardwert

Diese Kontrolle prüft, ob eine EC2 Amazon-Sicherheitsgruppe uneingeschränkten eingehenden Datenverkehr von nicht autorisierten Ports zulässt. Der Kontrollstatus wird wie folgt bestimmt:

- Wenn Sie den Standardwert für `authorizedTcpPorts` verwenden, schlägt die Steuerung fehl, wenn die Sicherheitsgruppe uneingeschränkten eingehenden Verkehr von einem anderen Port als den Ports 80 und 443 zulässt.
- Wenn Sie benutzerdefinierte Werte für `authorizedTcpPorts` oder `authorizedUdpPorts` angeben, schlägt die Steuerung fehl, wenn die Sicherheitsgruppe uneingeschränkten eingehenden Verkehr von einem nicht aufgelisteten Port zulässt.

Sicherheitsgruppen bieten eine statusabhängige Filterung von eingehendem und ausgehendem Netzwerkverkehr zu. AWS Sicherheitsgruppenregeln sollten dem Prinzip des Zugriffs mit den geringsten Rechten folgen. Uneingeschränkter Zugriff (IP-Adresse mit dem Suffix /0) erhöht die Wahrscheinlichkeit bössartiger Aktivitäten wie Hacking, denial-of-service Angriffe und Datenverlust.

Sofern ein Port nicht ausdrücklich zugelassen ist, sollte der Port den uneingeschränkten Zugriff verweigern.

Abhilfe

Informationen zum Ändern einer Sicherheitsgruppe finden Sie unter [Arbeiten mit Sicherheitsgruppen](#) im Amazon VPC-Benutzerhandbuch.

[EC2.19] Sicherheitsgruppen sollten keinen uneingeschränkten Zugriff auf Ports mit hohem Risiko zulassen

Verwandte Anforderungen: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), (1), NIST.800-53.r5 CA-9 (11), (16) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-7, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (21), (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), NIST.800-53.r5 SC-7 NIST.800-171.R2 3.1.3, NIST.800-53.r5 SC-7 NIST.800-171.R2 3.1.20, NIST.800-171.R2 3.13.1

Kategorie: Schützen > Eingeschränkter Netzwerkzugriff

Schweregrad: Kritisch

Art der Ressource: AWS::EC2::SecurityGroup

AWS Config Regel: [restricted-common-ports](#)(Die erstellte Regel ist vpc-sg-restricted-common-ports)

Art des Zeitplans: Ausgelöste und periodische Änderung

Parameter: "blockedPorts":

"20,21,22,23,25,110,135,143,445,1433,1434,3000,3306,3389,4333,5000,5432,5500,5600"
(nicht anpassbar)

Diese Kontrolle prüft, ob uneingeschränkter eingehender Verkehr für eine EC2 Amazon-Sicherheitsgruppe über die angegebenen Ports, die als risikoreich gelten, zugänglich ist. Diese Kontrolle schlägt fehl, wenn eine der Regeln in einer Sicherheitsgruppe eingehenden Datenverkehr von '0.0.0.0/0' oder ':::/0' zu diesen Ports zulässt.

Sicherheitsgruppen bieten eine zustandsorientierte Filterung von ein- und ausgehendem Netzwerkdatenverkehr von bzw. an AWS -Ressourcen. Uneingeschränkter Zugriff (0.0.0.0/0) erhöht die Wahrscheinlichkeit bössartiger Aktivitäten wie Hacking, Angriffe und Datenverlust. denial-of-service
Keine Sicherheitsgruppe sollte uneingeschränkten Zugriff auf die folgenden Ports zulassen:

- 20, 21 (FTP)
- 22 (SSH)
- 23 (Telnet)
- 25 (SMTP)
- 110 () POP3
- 135 (PRO STÜCK)
- 143 (IMAP)
- 445 (CIFS)
- 1433, 1434 (MSSQL)
- 3000 (Go-, Node.js- und Ruby-Frameworks für die Webentwicklung)
- 3306 (MySQL)
- 3389 (RDP)
- 4333 (ahsp)
- 5000 (Python-Frameworks für die Webentwicklung)
- 5432 (Postgresql)
- 5500 (1) fcp-addr-srvr
- 5601 (Armaturenbretter) OpenSearch
- 8080 (Proxy)
- 8088 (älterer HTTP-Port)
- 8888 (alternativer HTTP-Port)
- 9200 oder 9300 () OpenSearch

Abhilfe

Informationen zum Löschen von Regeln aus einer Sicherheitsgruppe finden [Sie unter Regeln aus einer Sicherheitsgruppe löschen](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.20] Beide VPN-Tunnel für eine AWS Site-to-Site VPN-Verbindung sollten aktiv sein

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5), NIST.800-171.R2 3.1.13, NIST.800-171.R2 3.1.20

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: AWS::EC2::VPNConnection

AWS Config -Regel: [vpc-vpn-2-tunnels-up](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Ein VPN-Tunnel ist eine verschlüsselte Verbindung, über die Daten vom Kundennetzwerk zu oder aus AWS einer AWS Site-to-Site VPN-Verbindung übertragen werden können. Jede VPN-Verbindung umfasst zwei VPN-Tunnel, die Sie für eine hohe Verfügbarkeit gleichzeitig verwenden können. Es ist wichtig, sicherzustellen, dass beide VPN-Tunnel für eine VPN-Verbindung verfügbar sind, um eine sichere und hochverfügbare Verbindung zwischen einer AWS VPC und Ihrem Remote-Netzwerk zu bestätigen.

Diese Steuerung überprüft, ob sich beide von VPN bereitgestellten AWS Site-to-Site VPN-Tunnel im UP-Status befinden. Die Steuerung schlägt fehl, wenn sich einer oder beide Tunnel im Status DOWN befinden.

Abhilfe

Informationen zum Ändern der VPN-Tunneloptionen finden Sie unter [Ändern der Site-to-Site VPN-Tunneloptionen](#) im AWS Site-to-Site VPN-Benutzerhandbuch.

[EC2.21] Das Netzwerk ACLs sollte keinen Zugang von 0.0.0.0/0 zu Port 22 oder Port 3389 zulassen

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.4.0/5.1, CIS AWS Foundations Benchmark v3.0.0/5.1, NIST.800-53.r5 AC-4 (21), (1), NIST.800-53.r5 CA-9 (21), NIST.800-53.r5 SC-7 (5) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-7, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 NIST.800-171.R2 3.1.3, NIST.800-171.r2 3.1.20, NIST.800-171.R2 3.13.1, PCI DSS v4.0.1/1.3.1

Kategorie: Schützen > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: AWS::EC2::NetworkAcl

AWS Config -Regel: [nacl-no-unrestricted-ssh-rdp](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Netzwerkzugriffskontrollliste (Network Access Control List, Netzwerk-ACL) uneingeschränkten Zugriff auf die Standard-TCP-Ports für SSH/RDP eingehenden Datenverkehr ermöglicht. Die Steuerung schlägt fehl, wenn der eingehende Netzwerk-ACL-Eintrag einen Quell-CIDR-Block von '0.0.0.0/0' oder ':::/0' für die TCP-Ports 22 oder 3389 zulässt. Das Steuerelement generiert keine Ergebnisse für eine Standard-Netzwerk-ACL.

Der Zugriff auf Remoteserveradministrationsports, wie Port 22 (SSH) und Port 3389 (RDP), sollte nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ressourcen innerhalb Ihrer VPC ermöglichen kann.

Abhilfe

Informationen zum Bearbeiten von Netzwerk-ACL-Verkehrsregeln finden Sie unter [Arbeiten mit dem Netzwerk ACLs](#) im Amazon VPC-Benutzerhandbuch.

[EC2.22] Ungenutzte EC2 Amazon-Sicherheitsgruppen sollten entfernt werden

Kategorie: Identifizieren > Bestand

Schweregrad: Mittel

Ressourcentyp: AWS::EC2::NetworkInterface, AWS::EC2::SecurityGroup

AWS Config -Regel: [ec2-security-group-attached-to-eni-periodic](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob Sicherheitsgruppen an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder an eine elastic network interface angehängt sind. Die Kontrolle schlägt fehl, wenn die Sicherheitsgruppe keiner EC2 Amazon-Instance oder einer elastic network interface zugeordnet ist.

 Important

Am 20. September 2023 hat Security Hub diese Kontrolle aus den Standards AWS Foundational Security Best Practices und NIST SP 800-53 Revision 5 entfernt. Diese Kontrolle ist weiterhin Teil des Service-Managed-Standards. AWS Control Tower
Dieses Steuerelement führt zu einer bestandenen Feststellung, ob Sicherheitsgruppen an EC2 Instances oder eine elastic network interface angehängt sind. In bestimmten Anwendungsfällen stellen nicht verknüpfte Sicherheitsgruppen jedoch kein Sicherheitsrisiko dar. Sie können andere EC2 Steuerelemente wie EC2 .2, EC2 .13, EC2 .14, EC2 .18 und .19 verwenden, um Ihre Sicherheitsgruppen zu überwachen. EC2

Abhilfe

Informationen zum Erstellen, Zuweisen und Löschen von Sicherheitsgruppen finden Sie unter [Sicherheitsgruppen für Ihre EC2 Instances](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.23] Amazon EC2 Transit Gateways sollte VPC-Anhangsanfragen nicht automatisch akzeptieren

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Hoch

Art der Ressource: AWS::EC2::TransitGateway

AWS Config -Regel: [ec2-transit-gateway-auto-vpc-attach-disabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob EC2 Transit-Gateways gemeinsam genutzte VPC-Anhänge automatisch akzeptieren. Diese Steuerung schlägt bei einem Transit-Gateway fehl, das automatisch gemeinsame VPC-Anhangsanforderungen akzeptiert.

Durch die Aktivierung wird ein Transit-Gateway so `AutoAcceptSharedAttachments` konfiguriert, dass es automatisch alle kontoübergreifenden VPC-Anhangsanforderungen akzeptiert, ohne die

Anfrage oder das Konto, von dem der Anhang stammt, zu überprüfen. Um den bewährten Methoden der Autorisierung und Authentifizierung zu folgen, empfehlen wir, diese Funktion zu deaktivieren, um sicherzustellen, dass nur autorisierte VPC-Anhangsanfragen akzeptiert werden.

Abhilfe

Informationen zum Ändern eines Transit-Gateways finden Sie unter [Modifizieren eines Transit-Gateways](#) im Amazon VPC Developer Guide.

[EC2.24] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden

Verwandte Anforderungen: NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2)

Kategorie: Identifizieren > Schwachstellen-, Patch- und Versionsverwaltung

Schweregrad: Mittel

Art der Ressource: AWS::EC2::Instance

AWS Config -Regel: [ec2-paravirtual-instance-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der Virtualisierungstyp einer EC2 Instanz paravirtuell ist. Die Steuerung schlägt fehl, wenn `virtualizationType` für die EC2 Instanz auf eingestellt ist. `paravirtual`

Linux Amazon Machine Images (AMIs) verwenden eine von zwei Arten der Virtualisierung: paravirtuelle (PV) oder virtuelle Hardware-Maschine (HVM). Die Hauptunterschiede zwischen PV und HVM AMIs bestehen in der Art und Weise, wie sie booten und ob sie spezielle Hardwareerweiterungen (CPU, Netzwerk und Speicher) für eine bessere Leistung nutzen können.

In der Vergangenheit hatten PV-Gäste in vielen Fällen eine bessere Leistung als HVM-Gäste, aber aufgrund der Verbesserungen bei der HVM-Virtualisierung und der Verfügbarkeit von PV-Treibern für HVM AMIs ist dies nicht mehr der Fall. Weitere Informationen finden Sie unter [Linux-AMI-Virtualisierungstypen](#) im EC2 Amazon-Benutzerhandbuch.

Abhilfe

Informationen zum Aktualisieren einer EC2 Instance auf einen neuen Instance-Typ finden Sie unter [Ändern des Instance-Typs](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.25] EC2 Amazon-Startvorlagen sollten Netzwerkschnittstellen nicht öffentlich IPs zuweisen

Verwandte Anforderungen: NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v4.0.1/1.4.4

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Hoch

Art der Ressource: AWS::EC2::LaunchTemplate

AWS Config -Regel: [ec2-launch-template-public-ip-disabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob EC2 Amazon-Startvorlagen so konfiguriert sind, dass Netzwerkschnittstellen beim Start öffentliche IP-Adressen zugewiesen werden. Die Steuerung schlägt fehl, wenn eine EC2 Startvorlage so konfiguriert ist, dass sie Netzwerkschnittstellen eine öffentliche IP-Adresse zuweist, oder wenn mindestens eine Netzwerkschnittstelle mit einer öffentlichen IP-Adresse vorhanden ist.

Eine öffentliche IP-Adresse ist eine Adresse, die über das Internet erreichbar ist. Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die mit diesen Netzwerkschnittstellen verknüpften Ressourcen möglicherweise vom Internet aus erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Workloads ermöglichen kann.

Abhilfe

Informationen zum Aktualisieren einer EC2 Startvorlage finden Sie unter [Ändern der Standardeinstellungen für die Netzwerkschnittstelle](#) im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

[EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt sein

Kategorie: Wiederherstellung > Ausfallsicherheit > Backups aktiviert

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-12, NIST.800-53.R5 SI-13 (5)

Schweregrad: Niedrig

Art der Ressource: AWS::EC2::Volume

AWS Config Regel: [ebs-resources-protected-by-backup-plan](#)

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
backupVaultLockCheck	Das Steuerelement ermittelt, ob der Parameter auf <code>true</code> gesetzt ist und die Ressource AWS Backup Vault Lock verwendet.	Boolesch	<code>true</code> oder <code>false</code>	Kein Standardwert

Diese Kontrolle bewertet, ob ein Amazon EBS-Volume im `in-use` Status durch einen Backup-Plan abgedeckt ist. Die Kontrolle schlägt fehl, wenn ein EBS-Volume nicht durch einen Backup-Plan abgedeckt ist. Wenn Sie den `backupVaultLockCheck` Parameter auf `true` setzen, ist die Steuerung nur erfolgreich, wenn das EBS-Volume in einem AWS Backup gesicherten Tresor gesichert ist.

Mithilfe von Backups können Sie sich nach einem Sicherheitsvorfall schneller erholen. Sie stärken auch die Widerstandsfähigkeit Ihrer Systeme. Wenn Sie Amazon EBS-Volumes in einen Backup-Plan aufnehmen, können Sie Ihre Daten vor unbeabsichtigtem Verlust oder Löschung schützen.

Abhilfe

Informationen zum Hinzufügen eines Amazon EBS-Volumes zu einem AWS Backup Backup-Plan finden Sie unter [Zuweisen von Ressourcen zu einem Backup-Plan](#) im AWS Backup Entwicklerhandbuch.

[EC2.33] EC2 Transit-Gateway-Anhänge sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Kennzeichnung

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::TransitGatewayAttachment`

AWS Config Regel: `tagged-ec2-transitgatewayattachment` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Diese Kontrolle prüft, ob ein Amazon EC2 Transit Gateway-Anhang Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind `requiredTagKeys`. Die Kontrolle schlägt fehl, wenn der Transit-Gateway-Anhang keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft die Steuerung nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn

der Transit-Gateway-Anhang mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `aws:` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der Allgemeinen AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EC2 Transit-Gateway-Anhang finden Sie unter [Taggen Sie Ihre EC2 Amazon-Ressourcen](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.34] Die Routentabellen für EC2 Transit-Gateways sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::TransitGatewayRouteTable`

AWS Config Regel: `tagged-ec2-transitgatewayroutetable` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon EC2 Transit Gateway-Routentabelle Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind `requiredTagKeys`. Die Steuerung schlägt fehl, wenn die Transit-Gateway-Routentabelle keine Tag-Schlüssel enthält oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Transit-Gateway-Routentabelle mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `aws:` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer EC2 Transit-Gateway-Routentabelle finden Sie unter [Taggen Ihrer EC2 Amazon-Ressourcen](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.35] EC2 Netzwerkschnittstellen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::EC2::NetworkInterface

AWS Config Regel: tagged-ec2-networkinterface (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
requiredTagKeys	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine EC2 Amazon-Netzwerkschnittstelle Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind `requiredTagKeys`. Die Steuerung schlägt fehl, wenn die Netzwerkschnittstelle keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Netzwerkschnittstelle mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer EC2 Netzwerkschnittstelle finden Sie unter [Taggen Ihrer EC2 Amazon-Ressourcen](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.36] EC2 Kunden-Gateways sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::CustomerGateway`

AWS Config Regel: `tagged-ec2-customergateway` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein EC2 Amazon-Kunden-Gateway Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind `requiredTagKeys`. Die Kontrolle schlägt fehl, wenn das Kunden-Gateway keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Kunden-Gateway mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginaws:` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien

für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EC2 Kunden-Gateway finden Sie unter [Taggen Sie Ihre EC2 Amazon-Ressourcen](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.37] EC2 Elastische IP-Adressen sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::EC2::EIP

AWS Config Regel: tagged-ec2-eip (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
requiredTagKeys	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS	Kein Standardwert

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen.	

Dieses Steuerelement prüft, ob eine Amazon EC2 Elastic IP-Adresse Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind `requiredTagKeys`. Die Steuerung schlägt fehl, wenn die Elastic IP-Adresse keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Elastic IP-Adresse mit keinem Schlüssel gekennzeichnet ist. System-Tags, die automatisch angewendet werden und mit `aws:*` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der Allgemeinen AWS-Referenz.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer EC2 Elastic IP-Adresse finden Sie unter [Taggen Ihrer EC2 Amazon-Ressourcen](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.38] EC2 Instances sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::EC2::Instance

AWS Config Regel: tagged-ec2-instance (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
requiredTagKeys	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine EC2 Amazon-Instance Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind `requiredTagKeys`. Die Steuerung schlägt fehl, wenn die Instance keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Instanz mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `aws:` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer EC2 Instance finden Sie unter [Taggen Ihrer EC2 Amazon-Ressourcen](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.39] EC2 Internet-Gateways sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::EC2::InternetGateway

AWS Config Regel: tagged-ec2-internetgateway (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein EC2 Amazon-Internet-Gateway Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind `requiredTagKeys`. Die Steuerung schlägt fehl, wenn das Internet-Gateway keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Internet-Gateway mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EC2 Internet-Gateway finden Sie unter [Taggen Sie Ihre EC2 Amazon-Ressourcen](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.40] EC2 NAT-Gateways sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::EC2::NatGateway

AWS Config Regel: tagged-ec2-natgateway (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
requiredTagKeys	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon EC2 Network Address Translation (NAT) -Gateway Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind `requiredTagKeys`. Die Steuerung schlägt fehl, wenn das NAT-Gateway keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das NAT-Gateway mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` , werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EC2 NAT-Gateway finden Sie unter [Taggen Ihrer EC2 Amazon-Ressourcen](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.41] Das EC2 Netzwerk ACLs sollte markiert sein

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::NetworkACL`

AWS Config Regel: `tagged-ec2-networkacl` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Diese Kontrolle prüft, ob eine EC2 Amazon-Netzwerkzugriffskontrollliste (Network ACL) Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind `requiredTagKeys`. Die Kontrolle schlägt fehl, wenn die Netzwerk-ACL keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Netzwerk-ACL mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginaws :` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien

für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer EC2 Netzwerk-ACL finden Sie unter [Taggen Ihrer EC2 Amazon-Ressourcen](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.42] EC2 Routing-Tabellen sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::EC2::RouteTable

AWS Config Regel: tagged-ec2-routetable (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
requiredTagKeys	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS	Kein Standardwert

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen.	

Dieses Steuerelement prüft, ob eine EC2 Amazon-Routing-Tabelle Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind `requiredTagKeys`. Die Steuerung schlägt fehl, wenn die Routing-Tabelle keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Routing-Tabelle mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer EC2 Routing-Tabelle finden Sie unter [Taggen Ihrer EC2 Amazon-Ressourcen](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.43] EC2 Sicherheitsgruppen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::EC2::SecurityGroup

AWS Config Regel: tagged-ec2-securitygroup (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
requiredTagKeys	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine EC2 Amazon-Sicherheitsgruppe Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind `requiredTagKeys`. Die Kontrolle schlägt fehl, wenn die Sicherheitsgruppe keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Sicherheitsgruppe mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginaws :` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer EC2 Sicherheitsgruppe finden Sie unter [Taggen Ihrer EC2 Amazon-Ressourcen](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.44] EC2 Subnetze sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::EC2::Subnet

AWS Config Regel: tagged-ec2-subnet (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein EC2 Amazon-Subnetz Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn das Subnetz keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel hat. `requiredTagKeys` Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Subnetz mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EC2 Subnetz finden Sie unter [Taggen Ihrer EC2 Amazon-Ressourcen](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.45] EC2 Volumen sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::EC2::Volume

AWS Config Regel: tagged-ec2-volume (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
requiredTagKeys	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein EC2 Amazon-Volume Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind `requiredTagKeys`. Die Steuerung schlägt fehl, wenn das Volume keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Volume mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `aws:*` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EC2 Band finden Sie unter [Taggen Sie Ihre EC2 Amazon-Ressourcen](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.46] Amazon VPCs sollte markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::EC2::VPC

AWS Config Regel: tagged-ec2-vpc (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
requiredTagKeys	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon Virtual Private Cloud (Amazon VPC) Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn die Amazon VPC keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Amazon VPC mit keinem Schlüssel gekennzeichnet ist. System-Tags, die automatisch angewendet werden und mit `beginaws:` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien

für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer VPC finden Sie unter [Taggen Ihrer EC2 Amazon-Ressourcen](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.47] Amazon VPC Endpoint Services sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::EC2::VPCEndpointService

AWS Config Regel: tagged-ec2-vpcendpointservice (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
requiredTagKeys	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS	Kein Standardwert

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen.	

Dieses Steuerelement prüft, ob ein Amazon VPC-Endpunktservice über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn der Endpunkt-Service keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Endpunktdienst mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der [Allgemeine AWS-Referenz](#).

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Amazon VPC-Endpunktservice finden Sie unter [Tags verwalten](#) im Abschnitt [Konfiguration eines Endpunktdienstes](#) des AWS PrivateLink Handbuchs.

[EC2.48] Amazon VPC-Flow-Logs sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::EC2::FlowLog

AWS Config Regel: tagged-ec2-flowlog (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
requiredTagKeys	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon VPC-Flow-Log Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn das Flow-Protokoll keine Tag-Schlüssel enthält oder wenn es nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Flow-Protokoll mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws:` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Amazon VPC-Flow-Protokoll finden Sie unter [Taggen eines Flow-Protokolls](#) im Amazon VPC-Benutzerhandbuch.

[EC2.49] Amazon VPC-Peering-Verbindungen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::VPCPeeringConnection`

AWS Config Regel: `tagged-ec2-vpcpeeringconnection` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon VPC-Peering-Verbindung Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind. `requiredTagKeys` Die Steuerung schlägt fehl, wenn die Peering-Verbindung keine Tag-Schlüssel hat oder wenn nicht alle im Parameter angegebenen Schlüssel vorhanden sind. `requiredTagKeys` Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Peering-Verbindung mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` , werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Amazon VPC-Peering-Verbindung finden Sie unter [Taggen Ihrer EC2 Amazon-Ressourcen](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.50] EC2 VPN-Gateways sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::EC2::VPNGateway

AWS Config Regel: tagged-ec2-vpngateway (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
requiredTagKeys	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon EC2 VPN-Gateway Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind `requiredTagKeys`. Die Steuerung schlägt fehl, wenn das VPN-Gateway keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das VPN-Gateway mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EC2 VPN-Gateway finden Sie unter [Taggen Sie Ihre EC2 Amazon-Ressourcen](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.51] EC2 Client-VPN-Endpunkte sollten die Client-Verbindungsprotokollierung aktiviert haben

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (12), (4), NIST.800-53.r5 AC-2 (26), (9), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 NIST.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8)

NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-9(7), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-4, NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8), NIST.800-171.R2 3.1.12, NIST.800-171.12, NIST.800-171.12 R2 3.1.20, PCI DSS v4.0.1/10.2.1

Kategorie: Identifizieren > Protokollierung

Schweregrad: Niedrig

Art der Ressource: AWS::EC2::ClientVpnEndpoint

AWS Config Regel: [ec2-client-vpn-connection-log-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für einen AWS Client VPN Endpunkt die Client-Verbindungsprotokollierung aktiviert ist. Die Steuerung schlägt fehl, wenn für den Endpunkt die Client-Verbindungsprotokollierung nicht aktiviert ist.

Client-VPN-Endpunkte ermöglichen Remote-Clients die sichere Verbindung zu Ressourcen in einer Virtual Private Cloud (VPC) in. AWS Verbindungsprotokolle ermöglichen es Ihnen, Benutzeraktivitäten auf dem VPN-Endpunkt zu verfolgen und bieten Transparenz. Wenn Sie die Verbindungsprotokollierung aktivieren, können Sie den Namen eines Protokolldatenstroms in der Protokollgruppe angeben. Wenn Sie keinen Protokollstream angeben, erstellt der Client-VPN-Dienst einen für Sie.

Abhilfe

Informationen zum Aktivieren der Verbindungsprotokollierung finden Sie unter [Aktivieren der Verbindungsprotokollierung für einen vorhandenen Client-VPN-Endpunkt](#) im AWS Client VPN Administratorhandbuch.

[EC2.52] EC2 Transit-Gateways sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::EC2::TransitGateway

AWS Config Regel: tagged-ec2-transitgateway (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Diese Steuerung prüft, ob ein Amazon EC2 Transit Gateway Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind `requiredTagKeys`. Die Kontrolle schlägt fehl, wenn das Transit-Gateway keine Tag-Schlüssel hat oder wenn es nicht über alle im Parameter angegebenen Schlüssel verfügt `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Transit-Gateway mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der Allgemeinen AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EC2 Transit-Gateway finden Sie unter [Taggen Sie Ihre EC2 Amazon-Ressourcen](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.53] EC2 Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 zu Remote-Serververwaltungsports zulassen

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/5.2, PCI DSS v4.0.1/1.3.1

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Sicherheitsgruppenkonfiguration

Schweregrad: Hoch

Art der Ressource: AWS::EC2::SecurityGroup

AWS Config -Regel: [vpc-sg-port-restriction-check](#)

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Standardwert
ipType	Die IP-Version	String	Nicht anpassbar	IPv4
restrictPorts	Liste der Ports, die eingehenden Datenverkehr ablehnen sollen	IntegerList	Nicht anpassbar	22, 3389

Diese Kontrolle prüft, ob eine EC2 Amazon-Sicherheitsgruppe den Zugriff von 0.0.0.0/0 zu den Remote-Serververwaltungsports (Ports 22 und 3389) zulässt. Die Kontrolle schlägt fehl, wenn die Sicherheitsgruppe den Zugriff von 0.0.0.0/0 auf Port 22 oder 3389 zulässt.

Sicherheitsgruppen bieten eine zustandsorientierte Filterung von ein- und ausgehendem Netzwerkdatenverkehr von bzw. an AWS -Ressourcen. Es wird empfohlen, dass keine Sicherheitsgruppe uneingeschränkten Zugriff auf Ports für die Remoteserververwaltung zulässt, z. B. SSH zu Port 22 und RDP zu Port 3389, wobei entweder die Protokolle TDP (6), UDP (17) oder ALL (-1) verwendet werden. Wenn der öffentliche Zugriff auf diese Ports zugelassen wird, erhöht sich die Angriffsfläche für Ressourcen und das Risiko einer Beeinträchtigung der Ressourcen.

Abhilfe

Informationen zum Aktualisieren einer EC2 Sicherheitsgruppenregel, um eingehenden Datenverkehr zu den angegebenen Ports zu verhindern, finden Sie unter [Sicherheitsgruppenregeln aktualisieren](#) im EC2 Amazon-Benutzerhandbuch. Nachdem Sie in der EC2 Amazon-Konsole eine Sicherheitsgruppe ausgewählt haben, wählen Sie Aktionen, Regeln für eingehenden Datenverkehr bearbeiten. Entfernen Sie die Regel, die den Zugriff auf Port 22 oder Port 3389 ermöglicht.

[EC2.54] EC2 Sicherheitsgruppen sollten keinen Zugriff von: :/0 zu Remote-Serveradministrationsports zulassen

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/5.3, PCI DSS v4.0.1/1.3.1

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Sicherheitsgruppenkonfiguration

Schweregrad: Hoch

Art der Ressource: AWS::EC2::SecurityGroup

AWS Config -Regel: [vpc-sg-port-restriction-check](#)

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Standardwert
ipType	Die IP-Version	String	Nicht anpassbar	IPv6
restrictPorts	Liste der Ports, die eingehenden Datenverkehr ablehnen sollen	IntegerList	Nicht anpassbar	22, 3389

Diese Steuerung prüft, ob eine EC2 Amazon-Sicherheitsgruppe den Zugriff von: :/0 zu den Remote-Serververwaltungsports (Ports 22 und 3389) zulässt. Die Kontrolle schlägt fehl, wenn die Sicherheitsgruppe den Zugang von: :/0 zu Port 22 oder 3389 zulässt.

Sicherheitsgruppen bieten eine zustandsorientierte Filterung von ein- und ausgehendem Netzwerkdatenverkehr von bzw. an AWS -Ressourcen. Es wird empfohlen, dass keine Sicherheitsgruppe uneingeschränkten Zugriff auf Ports für die Remoteserververwaltung zulässt, z. B. SSH zu Port 22 und RDP zu Port 3389, wobei entweder die Protokolle TDP (6), UDP (17) oder ALL (-1) verwendet werden. Wenn der öffentliche Zugriff auf diese Ports zugelassen wird, erhöht sich die Angriffsfläche für Ressourcen und das Risiko einer Beeinträchtigung der Ressourcen.

Abhilfe

Informationen zum Aktualisieren einer EC2 Sicherheitsgruppenregel, um eingehenden Datenverkehr zu den angegebenen Ports zu verhindern, finden Sie unter [Sicherheitsgruppenregeln aktualisieren](#) im EC2 Amazon-Benutzerhandbuch. Nachdem Sie in der EC2 Amazon-Konsole eine Sicherheitsgruppe ausgewählt haben, wählen Sie Aktionen, Regeln für eingehenden Datenverkehr bearbeiten. Entfernen Sie die Regel, die den Zugriff auf Port 22 oder Port 3389 ermöglicht.

[EC2.55] VPCs sollte mit einem Schnittstellenendpunkt für die ECR-API konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (4)

Kategorie: Schützen > Sicheres Zugriffsmanagement > Zugriffskontrolle

Schweregrad: Mittel

Ressourcentyp: AWS::EC2::VPC, AWS::EC2::VPCEndpoint

AWS Config -Regel: [vpc-endpoint-enabled](#)

Art des Zeitplans: Periodisch

Parameter:

Parameter	Erforderlich	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Standardwert
serviceNames	Erforderlich	Der Name des Dienstes, den das Steuerelement auswertet	String	Nicht anpassbar	ecr.api
vpcIds	Optional	Durch Kommas getrennte Liste von Amazon VPC IDs für VPC-Endpoints. Falls angegeben, schlägt die Steuerung fehl, wenn	StringList	Mit einer oder mehreren VPC anpassen IDs	Kein Standardwert

Parameter	Erforderlich	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
		die im serviceName Parameter angegebenen Dienste keinen dieser VPC-Endpunkte haben.			

Dieses Steuerelement prüft, ob eine von Ihnen verwaltete Virtual Private Cloud (VPC) über einen VPC-Schnittstellen-Endpunkt für die Amazon ECR-API verfügt. Die Steuerung schlägt fehl, wenn die VPC keinen VPC-Schnittstellen-Endpunkt für die ECR-API hat. Dieses Steuerelement bewertet Ressourcen in einem einzigen Konto.

AWS PrivateLink ermöglicht es Kunden, auf AWS hochverfügbare und skalierbare Weise auf Dienste zuzugreifen, auf denen gehostet wird, während der gesamte Netzwerkverkehr im AWS Netzwerk bleibt. Dienstbenutzer können privat auf Dienste zugreifen, die PrivateLink von ihrer VPC oder von ihren lokalen Standorten aus betrieben werden, ohne öffentliche IPs Dienste zu nutzen und ohne dass der Datenverkehr über das Internet übertragen werden muss.

Abhilfe

Informationen zur Konfiguration eines VPC-Endpunkts finden Sie unter [Zugreifen und AWS-Service Verwenden eines VPC-Endpunkts mit einer Schnittstelle](#) im AWS PrivateLink Handbuch.

[EC2.56] VPCs sollte mit einem Schnittstellenendpunkt für Docker Registry konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6 NIST.800-53.r5

SC-7, NIST.800-53.r5 SC-7 (11), (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (4)

Kategorie: Schützen > Sicheres Zugriffsmanagement > Zugriffskontrolle

Schweregrad: Mittel

Ressourcentyp: AWS::EC2::VPC, AWS::EC2::VPCEndpoint

AWS Config -Regel: [vpc-endpoint-enabled](#)

Art des Zeitplans: Periodisch

Parameter:

Parameter	Erforderlich	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
serviceNames	Erforderlich	Der Name des Dienstes, den das Steuerelement auswertet	String	Nicht anpassbar	ecr.dkr
vpcIds	Optional	Durch Kommas getrennte Liste von Amazon VPC IDs für VPC-Endpoints. Falls angegeben, schlägt	StringList	Mit einer oder mehreren VPC anpassen IDs	Kein Standardwert

Parameter	Erforderlich	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
		die Steuerung fehlt, wenn die im serviceName Parameter angegebenen Dienste keinen dieser VPC-Endpunkte haben.			

Dieses Steuerelement prüft, ob eine von Ihnen verwaltete Virtual Private Cloud (VPC) über einen VPC-Schnittstellen-Endpunkt für Docker Registry verfügt. Die Steuerung schlägt fehl, wenn die VPC keinen VPC-Schnittstellen-Endpunkt für Docker Registry hat. Dieses Steuerelement bewertet Ressourcen in einem einzigen Konto.

AWS PrivateLink ermöglicht es Kunden, auf AWS hochverfügbare und skalierbare Weise auf Dienste zuzugreifen, auf denen gehostet wird, während der gesamte Netzwerkverkehr im AWS Netzwerk bleibt. Dienstbenutzer können privat auf Dienste zugreifen, die PrivateLink von ihrer VPC oder von ihren lokalen Standorten aus betrieben werden, ohne öffentliche IPs Dienste zu nutzen und ohne dass der Datenverkehr über das Internet übertragen werden muss.

Abhilfe

Informationen zur Konfiguration eines VPC-Endpunkts finden Sie unter [Zugreifen und AWS-Service Verwenden eines VPC-Endpunkts mit einer Schnittstelle](#) im AWS PrivateLink Handbuch.

[EC2.57] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Kategorie: Schützen > Sicheres Zugriffsmanagement > Zugriffskontrolle

Schweregrad: Mittel

Ressourcentyp: AWS::EC2::VPC, AWS::EC2::VPCEndpoint

AWS Config -Regel: [vpc-endpoint-enabled](#)

Art des Zeitplans: Periodisch

Parameter:

Parameter	Erforderlich	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Standardwert
serviceNames	Erforderlich	Der Name des Dienstes, den das Steuerelement auswertet	String	Nicht anpassbar	ssm
vpcIds	Optional	Durch Kommas getrennte Liste von Amazon VPC IDs	StringList	Mit einer oder mehreren VPC anpassen IDs	Kein Standardwert

Parameter	Erforderlich	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
		für VPC-Endpunkte. Falls angegeben, schlägt die Steuerung fehl, wenn die im serviceName Parameter angegebenen Dienste keinen dieser VPC-Endpunkte haben.			

Dieses Steuerelement prüft, ob eine von Ihnen verwaltete Virtual Private Cloud (VPC) über einen VPC-Schnittstellen-Endpunkt verfügt. AWS Systems Manager Die Steuerung schlägt fehl, wenn die VPC keinen VPC-Schnittstellen-Endpunkt für Systems Manager hat. Dieses Steuerelement bewertet Ressourcen in einem einzigen Konto.

AWS PrivateLink ermöglicht es Kunden, auf AWS hochverfügbare und skalierbare Weise auf Dienste zuzugreifen, auf denen gehostet wird, während der gesamte Netzwerkverkehr im AWS Netzwerk bleibt. Dienstbenutzer können privat auf Dienste zugreifen, die PrivateLink von ihrer VPC oder von ihren lokalen Standorten aus betrieben werden, ohne öffentliche IPs Dienste zu nutzen und ohne dass der Datenverkehr über das Internet übertragen werden muss.

Abhilfe

Informationen zur Konfiguration eines VPC-Endpunkts finden Sie unter [Zugreifen und AWS-Service Verwenden eines VPC-Endpunkts mit einer Schnittstelle](#) im AWS PrivateLink Handbuch.

[EC2.58] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Kategorie: Schützen > Sicheres Zugriffsmanagement > Zugriffskontrolle

Schweregrad: Mittel

Ressourcentyp: AWS::EC2::VPC, AWS::EC2::VPCEndpoint

AWS Config -Regel: [vpc-endpoint-enabled](#)

Art des Zeitplans: Periodisch

Parameter:

Parameter	Erforderlich	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
serviceNames	Erforderlich	Der Name des Dienstes, den das Steuerelement auswertet	String	Nicht anpassbar	ssm-contacts
vpcIds	Optional	Durch Kommas getrennte	StringList	Mit einer oder mehreren	Kein Standardwert

Parameter	Erforderlich	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
		Liste von Amazon VPC IDs für VPC-Endpunkte. Falls angegeben, schlägt die Steuerung fehl, wenn die im <code>serviceName</code> Parameter angegebenen Dienste keinen dieser VPC-Endpunkte haben.		VPC anpassen IDs	

Dieses Steuerelement prüft, ob eine von Ihnen verwaltete Virtual Private Cloud (VPC) über einen VPC-Schnittstellen-Endpunkt für AWS Systems Manager Incident Manager-Kontakte verfügt. Die Steuerung schlägt fehl, wenn die VPC keinen VPC-Schnittstellen-Endpunkt für Systems Manager Incident Manager-Kontakte hat. Dieses Steuerelement bewertet Ressourcen in einem einzigen Konto.

AWS PrivateLink ermöglicht es Kunden, auf AWS hochverfügbare und skalierbare Weise auf Dienste zuzugreifen, auf denen gehostet wird, während der gesamte Netzwerkverkehr im AWS Netzwerk bleibt. Dienstbenutzer können privat auf Dienste zugreifen, die PrivateLink von ihrer VPC oder von

ihren lokalen Standorten aus betrieben werden, ohne öffentliche IPs Dienste zu nutzen und ohne dass der Datenverkehr über das Internet übertragen werden muss.

Abhilfe

Informationen zur Konfiguration eines VPC-Endpunkts finden Sie unter [Zugreifen und AWS-Service Verwenden eines VPC-Endpunkts mit einer Schnittstelle](#) im AWS PrivateLink Handbuch.

[EC2.60] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Kategorie: Schützen > Sicheres Zugriffsmanagement > Zugriffskontrolle

Schweregrad: Mittel

Ressourcentyp: AWS::EC2::VPC, AWS::EC2::VPCEndpoint

AWS Config -Regel: [vpc-endpoint-enabled](#)

Art des Zeitplans: Periodisch

Parameter:

Parameter	Erforderlich	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
serviceNames	Erforderlich	Der Name des Dienstes, den das Steuerelement auswertet	String	Nicht anpassbar	ssm-incidents

Parameter	Erforderlich	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
vpcIds	Optional	Durch Kommas getrennte Liste von Amazon VPC IDs für VPC-Endpunkte. Falls angegeben, schlägt die Steuerung fehl, wenn die im serviceName Parameter angegebenen Dienste keinen dieser VPC-Endpunkte haben.	StringList	Mit einer oder mehreren VPC anpassen IDs	Kein Standardwert

Dieses Steuerelement prüft, ob eine von Ihnen verwaltete Virtual Private Cloud (VPC) über einen VPC-Schnittstellen-Endpunkt für AWS Systems Manager Incident Manager verfügt. Die Steuerung schlägt fehl, wenn die VPC keinen VPC-Schnittstellen-Endpunkt für Systems Manager Incident Manager hat. Dieses Steuerelement bewertet Ressourcen in einem einzigen Konto.

AWS PrivateLink ermöglicht es Kunden, auf AWS hochverfügbare und skalierbare Weise auf Dienste zuzugreifen, auf denen gehostet wird, während der gesamte Netzwerkverkehr im AWS Netzwerk bleibt. Dienstbenutzer können privat auf Dienste zugreifen, die PrivateLink von ihrer VPC oder von ihren lokalen Standorten aus betrieben werden, ohne öffentliche IPs Dienste zu nutzen und ohne dass der Datenverkehr über das Internet übertragen werden muss.

Abhilfe

Informationen zur Konfiguration eines VPC-Endpunkts finden Sie unter [Zugreifen und AWS-Service Verwenden eines VPC-Endpunkts mit einer Schnittstelle](#) im AWS PrivateLink Handbuch.

[EC2.170] EC2 Startvorlagen sollten Instance Metadata Service Version 2 () verwenden IMDSv2

Verwandte Anforderungen: PCI DSS v4.0.1/2.2.6

Kategorie: Schützen > Netzwerksicherheit

Schweregrad: Niedrig

Art der Ressource: AWS::EC2::LaunchTemplate

AWS Config -Regel: [ec2-launch-template-imdsv2-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine EC2 Amazon-Startvorlage mit Instance Metadata Service Version 2 (IMDSv2) konfiguriert ist. Die Steuerung schlägt fehl, wenn sie auf gesetzt `HttpTokens istoptional`.

Das Ausführen von Ressourcen auf unterstützten Softwareversionen gewährleistet optimale Leistung, Sicherheit und Zugriff auf die neuesten Funktionen. Regelmäßige Updates schützen vor Sicherheitslücken und sorgen so für ein stabiles und effizientes Benutzererlebnis.

Abhilfe

Informationen IMDSv2 zur Anforderung einer EC2 Startvorlage finden [Sie unter Konfiguration der Optionen für den Instance-Metadaten-Service](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.171] Bei EC2 VPN-Verbindungen sollte die Protokollierung aktiviert sein

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/5.3, PCI DSS v4.0.1/10.4.2

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS::EC2::VPNConnection

AWS Config -Regel: [ec2-vpn-connection-logging-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob bei einer AWS Site-to-Site VPN-Verbindung Amazon CloudWatch Logs für beide Tunnel aktiviert ist. Die Kontrolle schlägt fehl, wenn bei einer Site-to-Site VPN-Verbindung CloudWatch Logs nicht für beide Tunnel aktiviert sind.

AWS Site-to-Site VPN-Protokolle bieten Ihnen einen tieferen Einblick in Ihre Site-to-Site VPN-Bereitstellungen. Mit dieser Funktion haben Sie Zugriff auf Site-to-Site VPN-Verbindungsprotokolle, die Einzelheiten zur Einrichtung eines IP-Security-Tunnels (IPsec), zu IKE-Verhandlungen (Internet Key Exchange) und zu DPD-Protokollnachrichten (Dead Peer Detection) enthalten. Site-to-Site VPN-Protokolle können in CloudWatch Logs veröffentlicht werden. Diese Funktion bietet Kunden eine einzige konsistente Möglichkeit, auf detaillierte Protokolle für all ihre Site-to-Site VPN-Verbindungen zuzugreifen und diese zu analysieren.

Abhilfe

Informationen zur Aktivierung der Tunnelprotokollierung für eine EC2 [AWS Site-to-Site VPN-Verbindung finden Sie unter VPN-Protokolle](#) im AWS Site-to-Site VPN-Benutzerhandbuch.

[EC2.172] Die Einstellungen von EC2 VPC Block Public Access sollten den Internet-Gateway-Verkehr blockieren

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Mittel

Art der Ressource: AWS::EC2::VPCBlockPublicAccessOptions

AWS Config Regel: ec2-vpc-bpa-internet-gateway-blocked (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
vpcBpaInternetGatewayBlockMode	Zeichenkettenwert des VPC BPA-Optionsmodus.	Enum	block-bidirectional, block-ingress	Kein Standardwert

Dieses Steuerelement prüft, ob die Amazon EC2 VPC Block Public Access (BPA) -Einstellungen so konfiguriert sind, dass der Internet-Gateway-Verkehr für den gesamten Amazon VPCs in der blockiert wird. AWS-Konto Die Steuerung schlägt fehl, wenn die VPC BPA-Einstellungen nicht so konfiguriert sind, dass sie den Internet-Gateway-Verkehr blockieren. Damit die Kontrolle erfolgreich ist, InternetGatewayBlockMode muss der VPC BPA auf oder gesetzt sein block-bidirectional. block-ingress Wenn der Parameter angegeben vpcBpaInternetGatewayBlockMode wird, wird die Steuerung nur erfolgreich ausgeführt, wenn der VPC BPA-Wert für InternetGatewayBlockMode mit dem Parameter übereinstimmt.

Wenn Sie die VPC-BPA-Einstellungen für Ihr Konto in einer Region konfigurieren, können Sie verhindern, dass Ressourcen in VPCs und Subnetzen, die Sie besitzen, in dieser Region über Internet-Gateways und Internet-Gateways nur für ausgehenden Datenverkehr erreichen oder vom Internet aus erreicht werden. Wenn Sie bestimmte VPCs Subnetze benötigen, um auf das Internet zuzugreifen oder über das Internet erreichbar zu sein, können Sie diese ausschließen, indem Sie VPC-BPA-Ausschlüsse konfigurieren. Anweisungen zum Erstellen und Löschen von Ausschlüssen finden Sie unter [Ausnahmen erstellen und löschen](#) im Amazon VPC-Benutzerhandbuch.

Abhilfe

Informationen zur Aktivierung von bidirektionalem BPA auf Kontoebene finden Sie unter [Bidirektionalen BPA-Modus für Ihr Konto aktivieren](#) im Amazon VPC-Benutzerhandbuch.

Informationen zum Aktivieren von BPA nur für eingehenden Datenverkehr finden Sie unter [Ändern des VPC-BPA-Modus](#) auf Nur eingehenden Datenverkehr. Informationen zur Aktivierung von VPC BPA auf Organisationsebene finden Sie unter [Aktivieren von VPC BPA auf Organisationsebene](#).

[EC2.173] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: AWS::EC2::SpotFleet

AWS Config -Regel: [ec2-spot-fleet-request-ct-encryption-at-rest](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob eine Amazon EC2 Spot Fleet-Anfrage, die Startparameter festlegt, so konfiguriert ist, dass die Verschlüsselung für alle Amazon Elastic Block Store (Amazon EBS) - Volumes (Amazon EBS) aktiviert wird, die an EC2 Instances angehängt sind. Die Kontrolle schlägt fehl, wenn die Spot-Fleet-Anfrage Startparameter spezifiziert und die Verschlüsselung für ein oder mehrere in der Anfrage angegebene EBS-Volumes nicht aktiviert.

Für eine zusätzliche Sicherheitsebene sollten Sie die Verschlüsselung für Amazon EBS-Volumes aktivieren. Verschlüsselungsvorgänge finden dann auf den Servern statt, die EC2 Amazon-Instances hosten, wodurch die Sicherheit sowohl der Daten im Ruhezustand als auch der Daten während der Übertragung zwischen einer Instance und dem angeschlossenen EBS-Speicher gewährleistet wird. Die Amazon EBS-Verschlüsselung ist eine einfache Verschlüsselungslösung für EBS-Ressourcen, die mit Ihren EC2 Instances verknüpft sind. Mit der EBS-Verschlüsselung müssen Sie Ihre eigene Schlüsselverwaltungsinfrastruktur nicht aufbauen, warten und sichern. Die EBS-Verschlüsselung wird AWS KMS keys bei der Erstellung verschlüsselter Volumes verwendet.

Hinweise

Dieses Steuerelement generiert keine Ergebnisse für Amazon EC2 Spot-Flotte-Anfragen, die Startvorlagen verwenden. Es generiert auch keine Ergebnisse für Spot-Flotte-Anfragen, die nicht explizit einen Wert für den encrypted Parameter angeben.

Am 23. Juli 2025 änderte Security Hub den Titel dieses Steuerelements. Zuvor lautete der Titel dieses Steuerelements: EC2 Spot Fleet requests should enable encryption for attached EBS volumes. Der neue Titel spiegelt genauer wider, dass das Steuerelement nur Spot-Flottenanfragen überprüft, die Startparameter angeben.

Abhilfe

Es gibt keine direkte Möglichkeit, ein vorhandenes, unverschlüsseltes Amazon EBS-Volume zu verschlüsseln. Sie können ein neues Volume nur verschlüsseln, wenn Sie es erstellen.

Wenn Sie jedoch die Verschlüsselung standardmäßig aktivieren, verschlüsselt Amazon EBS neue Volumes mithilfe Ihres Standardschlüssels für die EBS-Verschlüsselung. Wenn Sie die Verschlüsselung nicht standardmäßig aktivieren, können Sie die Verschlüsselung aktivieren, wenn Sie ein einzelnes Volume erstellen. In beiden Fällen können Sie den Standardschlüssel für die EBS-Verschlüsselung außer Kraft setzen und einen vom Kunden verwalteten AWS KMS key Schlüssel auswählen. Weitere Informationen zur EBS-Verschlüsselung finden Sie unter [Amazon EBS-Verschlüsselung](#) im Amazon EBS-Benutzerhandbuch.

Informationen zum Erstellen einer Amazon EC2 Spot-Flotte-Anfrage finden [Sie unter Erstellen einer Spot-Flotte](#) im Amazon Elastic Compute Cloud-Benutzerhandbuch.

[EC2.174] EC2 DHCP-Optionssätze sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::EC2::DHCPOptions

AWS Config -Regel: [ec2-dhcp-options-tagged](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Eine Liste der Tag-Schlüssel vom Typ „“, die einer ausgewerteten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon EC2 DHCP-Optionssatz die durch den `requiredKeyTags` Parameter angegebenen Tag-Schlüssel enthält. Die Steuerung schlägt fehl, wenn der Optionssatz keine Tag-Schlüssel oder nicht alle im `requiredKeyTags` Parameter angegebenen Schlüssel enthält. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Optionssatz keine Tag-Schlüssel enthält. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws:` Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im [Tagging AWS Resources and Tag](#) Editor User Guide.

 Note

Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Amazon EC2 DHCP-Optionssatz finden Sie unter [Taggen Ihrer EC2 Amazon-Ressourcen](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.175] EC2 Startvorlagen sollten mit Tags versehen sein

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::EC2::LaunchTemplate

AWS Config -Regel: [ec2-launch-template-tagged](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
requiredKeyTags	Eine Liste der Tag-Schlüssel vom Typ „“, die einer ausgewerteten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine EC2 Amazon-Startvorlage die durch den `requiredKeyTags` Parameter angegebenen Tag-Schlüssel enthält. Die Steuerung schlägt fehl, wenn die Startvorlage keine Tag-Schlüssel oder nicht alle im `requiredKeyTags` Parameter angegebenen Schlüssel enthält. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Startvorlage keine Tagschlüssel enthält. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws` : Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im [Tagging AWS Resources and Tag](#) Editor User Guide.

 Note

Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer EC2 Amazon-Startvorlage finden Sie unter [Taggen Ihrer EC2 Amazon-Ressourcen](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.176] EC2 Präfixlisten sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::PrefixList`

AWS Config -Regel: [ec2-prefix-list-tagged](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Eine Liste der Tag-Schlüssel vom Typ „“, die einer ausgewerteten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine EC2 Amazon-Präfixliste die durch den `requiredKeyTags` Parameter angegebenen Tag-Schlüssel enthält. Das Steuerelement schlägt fehl, wenn die Präfixliste keine Tag-Schlüssel oder nicht alle im `requiredKeyTags` Parameter angegebenen Schlüssel enthält. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Präfixliste keine Tagschlüssel enthält. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws:` Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im [Tagging AWS Resources and Tag](#) Editor User Guide.

 Note

Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer EC2 Amazon-Präfixliste finden Sie unter [Taggen Ihrer EC2 Amazon-Ressourcen](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.177] EC2 Traffic Mirror-Sitzungen sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::TrafficMirrorSession`

AWS Config -Regel: [ec2-traffic-mirror-session-tagged](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Eine Liste der Tag-Schlüssel vom Typ „“, die einer ausgewerteten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon EC2 Traffic Mirror-Sitzung die durch den `requiredKeyTags` Parameter angegebenen Tag-Schlüssel enthält. Die Steuerung schlägt fehl, wenn die Sitzung keine Tag-Schlüssel oder nicht alle im `requiredKeyTags` Parameter angegebenen Schlüssel hat. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Sitzung keine Tagschlüssel hat. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws` : Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im [Tagging AWS Resources and Tag](#) Editor User Guide.

 Note

Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Amazon EC2 Traffic Mirror-Sitzung finden Sie unter [Taggen Ihrer EC2 Amazon-Ressourcen](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.178] Filter für EC2 Verkehrsspiegel sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::TrafficMirrorFilter`

AWS Config -Regel: [ec2-traffic-mirror-filter-tagged](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Eine Liste der Tag-Schlüssel vom Typ „“, die einer ausgewerteten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein EC2 Amazon-Traffic-Mirror-Filter über die im `requiredKeyTags` Parameter angegebenen Tag-Schlüssel verfügt. Das Steuerelement schlägt fehl, wenn der Filter keine Tag-Schlüssel oder nicht alle im `requiredKeyTags` Parameter angegebenen Schlüssel hat. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Filter keine Tagschlüssel hat. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws:` Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im [Tagging AWS Resources and Tag](#) Editor User Guide.

 Note

Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Amazon EC2 Traffic Mirror-Filter finden Sie unter [Taggen Ihrer EC2 Amazon-Ressourcen](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.179] EC2 Traffic-Spiegel-Ziele sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::TrafficMirrorTarget`

AWS Config -Regel: [ec2-traffic-mirror-target-tagged](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Eine Liste der Tag-Schlüssel vom Typ „“, die einer ausgewerteten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein EC2 Amazon-Traffic-Mirror-Ziel über die im `requiredKeyTags` Parameter angegebenen Tag-Schlüssel verfügt. Die Steuerung schlägt fehl, wenn das Ziel keine Tag-Schlüssel oder nicht alle im `requiredKeyTags` Parameter angegebenen Schlüssel hat. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Ziel keine Tagschlüssel hat. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws :` Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im [Tagging AWS Resources and Tag](#) Editor User Guide.

 Note

Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Amazon EC2 Traffic Mirror-Target finden Sie unter [Taggen Ihrer EC2 Amazon-Ressourcen](#) im EC2 Amazon-Benutzerhandbuch.

[EC2.180] Bei EC2 Netzwerkschnittstellen sollte die source/destination Überprüfung aktiviert sein

Kategorie: Schützen > Netzwerksicherheit

Schweregrad: Mittel

Art der Ressource: AWS::EC2::NetworkInterface

AWS Config -Regel: [ec2-enis-source-destination-check-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die source/destination Prüfung für ein Amazon EC2 elastic network interface (ENI) aktiviert ist, das von Benutzern verwaltet wird. Die Steuerung schlägt fehl, wenn die source/destination Prüfung für das benutzerverwaltete ENI deaktiviert ist. Dieses Steuerelement überprüft nur die folgenden Typen von ENIs:aws_codestar_connections_managed,branch,efa, interfacelambda, undquicksight.

Source/destination checking for Amazon EC2 instances and attached ENIs should be enabled and configured consistently across your EC2 instances. Each ENI has its own setting for source/destination checks. If source/destination checking is enabled, Amazon EC2 enforces source/destinationAdressvalidierung, die sicherstellt, dass eine Instance entweder die Quelle oder das Ziel jeglichen Datenverkehrs ist, den sie empfängt. Dies bietet eine zusätzliche Netzwerksicherheitsebene, indem verhindert wird, dass Ressourcen unbeabsichtigten Datenverkehr verarbeiten, und IP-Adress-Spoofing verhindert wird.

Note

Wenn Sie eine EC2 Instance als NAT-Instance verwenden und die source/destination Überprüfung auf ihre ENI deaktiviert haben, können Sie stattdessen ein [NAT-Gateway](#) verwenden.

Abhilfe

Informationen zum Aktivieren von source/destination Prüfungen für ein Amazon EC2 ENI finden Sie unter [Ändern von Netzwerkschnittstellenattributen](#) im EC2 Amazon-Benutzerhandbuch.

Security Hub-Steuerelemente für Auto Scaling

Diese Security Hub Hub-Kontrollen bewerten den Service und die Ressourcen von Amazon EC2 Auto Scaling.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[AutoScaling.1] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden

Verwandte Anforderungen: PCI DSS v3.2.1/2.2, NIST.800-53.R5 CP-2 (2) NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-2

Kategorie: Identifizieren > Bestand

Schweregrad: Niedrig

Art der Ressource: AWS::AutoScaling::AutoScalingGroup

AWS Config -Regel: [autoscaling-group-elb-healthcheck-required](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Amazon EC2 Auto Scaling Scaling-Gruppe, die einem Load Balancer zugeordnet ist, Elastic Load Balancing (ELB) -Zustandsprüfungen verwendet. Die Steuerung schlägt fehl, wenn die Auto Scaling Scaling-Gruppe keine ELB-Zustandsprüfungen verwendet.

ELB-Zustandsprüfungen stellen sicher, dass eine Auto Scaling Scaling-Gruppe den Zustand einer Instance anhand zusätzlicher Tests ermitteln kann, die vom Load Balancer bereitgestellt werden. Die Verwendung von Elastic Load Balancing Health Checks trägt auch dazu bei, die Verfügbarkeit von Anwendungen zu unterstützen, die EC2 Auto Scaling Scaling-Gruppen verwenden.

Abhilfe

Informationen zum Hinzufügen von Elastic Load Balancing Balancing-Zustandsprüfungen finden [Sie unter Elastic Load Balancing Balancing-Zustandsprüfungen hinzufügen](#) im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

[AutoScaling.2] Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2(2), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: AWS::AutoScaling::AutoScalingGroup

AWS Config -Regel: [autoscaling-multiple-az](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert	
minAvailabilityZones	Mindestanzahl von Availability Zones	Enum	2, 3, 4, 5, 6	2	

Dieses Steuerelement prüft, ob eine Amazon EC2 Auto Scaling Scaling-Gruppe mindestens die angegebene Anzahl von Availability Zones (AZs) umfasst. Die Steuerung schlägt fehl, wenn eine Auto Scaling Scaling-Gruppe nicht mindestens die angegebene Anzahl von umfasst AZs. Sofern Sie keinen benutzerdefinierten Parameterwert für die Mindestanzahl von angeben AZs, verwendet Security Hub den Standardwert AZs 2.

Eine Auto Scaling Scaling-Gruppe, die sich nicht über mehrere erstreckt, AZs kann keine Instances in einer anderen AZ starten, um dies zu kompensieren, wenn die konfigurierte einzelne AZ nicht mehr verfügbar ist. In einigen Anwendungsfällen kann jedoch eine Auto Scaling Scaling-Gruppe mit einer einzigen Availability Zone bevorzugt werden, z. B. bei Batch-Jobs oder wenn die Inter-AZ-Übertragungskosten auf ein Minimum beschränkt werden müssen. In solchen Fällen können Sie diese Steuerung deaktivieren oder ihre Ergebnisse unterdrücken.

Abhilfe

Informationen zum Hinzufügen AZs zu einer vorhandenen Auto Scaling Scaling-Gruppe finden Sie unter [Availability Zones hinzufügen und entfernen](#) im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

[AutoScaling.3] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2 Instances so konfigurieren, dass sie Instance Metadata Service Version 2 (IMDSv2) benötigen

Verwandte Anforderungen: NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), (7), NIST.800-53.r5 AC-3 NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 AC-6, NIST.800-53.R5 CM-2, PCI DSS v4.0.1/2.2.6

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Hoch

Art der Ressource: AWS::AutoScaling::LaunchConfiguration

AWS Config -Regel: [autoscaling-launchconfig-requires-imdsv2](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob IMDSv2 es auf allen Instances aktiviert ist, die von Amazon EC2 Auto Scaling Scaling-Gruppen gestartet wurden. Die Steuerung schlägt fehl, wenn die Version des Instance Metadata Service (IMDS) nicht in der Startkonfiguration enthalten ist oder als konfiguriert ist `token optional`, was eine Einstellung ist, die entweder IMDSv1 oder IMDSv2 zulässt.

IMDS stellt Daten über Ihre Instance bereit, die Sie verwenden können, um die laufende Instance zu konfigurieren oder zu verwalten.

Version 2 des IMDS fügt neue Schutzmaßnahmen hinzu, die in nicht verfügbar waren, um Ihre Instances weiter IMDSv1 zu schützen. EC2

Abhilfe

Eine Auto Scaling Scaling-Gruppe ist jeweils einer Startkonfiguration zugeordnet. Sie können eine Startkonfiguration nicht ändern, nachdem Sie sie erstellt haben. Um die Startkonfiguration für eine Auto Scaling Scaling-Gruppe zu ändern, verwenden Sie eine vorhandene Startkonfiguration als Grundlage für eine neue Startkonfiguration mit IMDSv2 enabled. Weitere Informationen finden [Sie unter Konfigurieren von Instance-Metadatenoptionen für neue Instances](#) im EC2 Amazon-Benutzerhandbuch.

[AutoScaling.4] Die Auto Scaling Scaling-Gruppenstartkonfiguration sollte kein Metadaten-Response-Hop-Limit größer als 1 haben

Important

Security Hub hat diese Kontrolle im April 2024 eingestellt. Weitere Informationen finden Sie unter [Änderungsprotokoll für Security Hub CSPM-Steuerelemente](#).

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2)

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Hoch

Art der Ressource: AWS::AutoScaling::LaunchConfiguration

AWS Config -Regel: [autoscaling-launch-config-hop-limit](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement überprüft die Anzahl der Netzwerk-Hops, die ein Metadaten-Token zurücklegen kann. Die Steuerung schlägt fehl, wenn das Limit für Metadaten-Antwort-Hops größer als ist1.

Der Instance Metadata Service (IMDS) stellt Metadateninformationen zu einer EC2 Amazon-Instance bereit und ist für die Anwendungskonfiguration nützlich. Die Beschränkung der PUT HTTP-Antwort für den Metadaten-Service auf nur die EC2 Instance schützt das IMDS vor unbefugter Nutzung.

Das TTL-Feld (Time To Live) im IP-Paket wird bei jedem Hop um eins reduziert. Diese Reduzierung kann verwendet werden, um sicherzustellen, dass das Paket nicht nach außen EC2 transportiert wird. IMDSv2 schützt EC2 Instanzen, die möglicherweise als offene Router, Layer-3-Firewalls, Tunnel oder NAT-Geräte falsch konfiguriert wurden, wodurch verhindert wird, dass unbefugte Benutzer Metadaten abrufen. VPNs Mit kann die PUT Antwort IMDSv2, die das geheime Token enthält, die Instanz nicht verlassen, da das standardmäßige Antwort-Hop-Limit für Metadaten auf festgelegt ist. 1 Wenn dieser Wert jedoch größer als ist1, kann das Token die EC2 Instance verlassen.

Abhilfe

Informationen zum Ändern des Metadaten-Response-Hop-Limits für eine bestehende Startkonfiguration finden Sie unter [Ändern von Instance-Metadaten-Optionen für bestehende Instances](#) im EC2 Amazon-Benutzerhandbuch.

[Autoscaling.5] EC2 Amazon-Instances, die mit Auto Scaling Scaling-Gruppenstartkonfigurationen gestartet wurden, sollten keine öffentlichen IP-Adressen haben

Verwandte Anforderungen: NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v4.0.1/1.4.4

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Hoch

Art der Ressource: AWS::AutoScaling::LaunchConfiguration

AWS Config -Regel: [autoscaling-launch-config-public-ip-disabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die zugehörige Startkonfiguration einer Auto Scaling Scaling-Gruppe den Instances der Gruppe eine [öffentliche IP-Adresse](#) zuweist. Die Steuerung schlägt fehl, wenn die zugehörige Startkonfiguration eine öffentliche IP-Adresse zuweist.

EC2 Amazon-Instances in einer Auto Scaling Scaling-Gruppenstartkonfiguration sollten keine zugeordnete öffentliche IP-Adresse haben, außer in begrenzten Randfällen. EC2 Amazon-Instances sollten nur hinter einem Load Balancer zugänglich sein, anstatt direkt dem Internet ausgesetzt zu sein.

Abhilfe

Eine Auto Scaling Scaling-Gruppe ist jeweils einer Startkonfiguration zugeordnet. Sie können eine Startkonfiguration nicht ändern, nachdem Sie sie erstellt haben. Um die Startkonfiguration einer

Auto-Scaling-Gruppe zu ändern, verwenden Sie eine vorhandene Startkonfiguration als Grundlage für eine neue Startkonfiguration. Aktualisieren Sie dann die Auto-Scaling-Gruppe so, dass die neue Startkonfiguration verwendet wird. [step-by-stepAnweisungen](#) finden Sie unter [Ändern der Startkonfiguration für eine Auto Scaling Group](#) im Amazon EC2 Auto Scaling Benutzerhandbuch. Wählen Sie bei der Erstellung der neuen Startkonfiguration unter Zusätzliche Konfiguration für Erweiterte Details und IP-Adresstyp die Option Keinen Instances eine öffentliche IP-Adresse zuweisen aus.

Nachdem Sie die Startkonfiguration geändert haben, startet Auto Scaling neue Instances mit den neuen Konfigurationsoptionen. Bestehende Instanzen sind nicht betroffen. Um eine bestehende Instance zu aktualisieren, empfehlen wir Ihnen, Ihre Instance zu aktualisieren oder die automatische Skalierung zuzulassen, um ältere Instances auf der Grundlage Ihrer Kündigungsrichtlinien schrittweise durch neuere Instances zu ersetzen. Weitere Informationen zur Aktualisierung von Auto Scaling Instances finden Sie unter [Auto Scaling Instances aktualisieren](#) im Amazon EC2 Auto Scaling Benutzerhandbuch.

[AutoScaling.6] Auto Scaling Groups sollten mehrere Instance-Typen in mehreren Availability Zones verwenden

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2(2), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: AWS::AutoScaling::AutoScalingGroup

AWS Config -Regel: [autoscaling-multiple-instance-types](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Amazon EC2 Auto Scaling Group mehrere Instance-Typen verwendet. Die Steuerung schlägt fehl, wenn für die Auto Scaling Group nur ein Instanztyp definiert ist.

Sie können die Verfügbarkeit verbessern, indem Sie Ihre Anwendung auf mehreren Instance-Typen bereitstellen, die in mehreren Availability Zones ausgeführt werden. Security Hub empfiehlt die Verwendung mehrerer Instanztypen, damit die Auto Scaling Group einen anderen Instance-

Typ starten kann, wenn die Instance-Kapazität in den von Ihnen ausgewählten Availability Zones nicht ausreicht.

Abhilfe

Informationen zum Erstellen einer Auto Scaling Scaling-Gruppe mit mehreren Instance-Typen finden Sie unter [Auto Scaling Scaling-Gruppen mit mehreren Instance-Typen und Kaufoptionen](#) im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

[AutoScaling.9] Amazon EC2 Auto Scaling Scaling-Gruppen sollten EC2 Amazon-Startvorlagen verwenden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2)

Kategorie: Identifizieren > Ressourcenkonfiguration

Schweregrad: Mittel

Art der Ressource: AWS::AutoScaling::AutoScalingGroup

AWS Config -Regel: [autoscaling-launch-template](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Amazon EC2 Auto Scaling Scaling-Gruppe anhand einer EC2 Startvorlage erstellt wurde. Diese Kontrolle schlägt fehl, wenn eine Amazon EC2 Auto Scaling Scaling-Gruppe nicht mit einer Startvorlage erstellt wird oder wenn keine Startvorlage in einer Richtlinie für gemischte Instanzen angegeben ist.

Eine EC2 Auto Scaling Scaling-Gruppe kann entweder aus einer EC2 Startvorlage oder einer Startkonfiguration erstellt werden. Die Verwendung einer Startvorlage zur Erstellung einer Auto Scaling Scaling-Gruppe stellt jedoch sicher, dass Sie Zugriff auf die neuesten Funktionen und Verbesserungen haben.

Abhilfe

Informationen zum Erstellen einer Auto Scaling Scaling-Gruppe mit einer EC2 Startvorlage finden Sie unter [Erstellen einer Auto Scaling Scaling-Gruppe mithilfe einer Startvorlage](#) im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch. Informationen zum Ersetzen einer Startkonfiguration durch

eine Startvorlage finden Sie unter [Ersetzen einer Startkonfiguration durch eine Startvorlage](#) im EC2 Amazon-Benutzerhandbuch.

[AutoScaling.10] EC2 Auto Scaling Scaling-Gruppen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::AutoScaling::AutoScalingGroup

AWS Config Regel: tagged-autoscaling-autoscalinggroup (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
requiredTagKeys	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon EC2 Auto Scaling Scaling-Gruppe Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind `requiredTagKeys`. Die Steuerung schlägt fehl, wenn die Auto Scaling Scaling-Gruppe keine Tagschlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Auto Scaling Scaling-Gruppe mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `aws:` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Auto Scaling Scaling-Gruppe finden Sie unter [Tag Auto Scaling Scaling-Gruppen und -Instances](#) im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

Security Hub-Steuerelemente für Amazon ECR

Diese Security Hub Hub-Kontrollen bewerten den Service und die Ressourcen von Amazon Elastic Container Registry (Amazon ECR).

Diese Kontrollen sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein

Verwandte Anforderungen: NIST.800-53.r5 RA-5, PCI DSS v4.0.1/6.2.3, PCI DSS v4.0.1/6.2.4

Kategorie: Identifizieren > Sicherheitslücken-, Patch- und Versionsverwaltung

Schweregrad: Hoch

Art der Ressource: AWS::ECR::Repository

AWS Config -Regel: [ecr-private-image-scanning-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob für ein privates Amazon ECR-Repository das Scannen von Bildern konfiguriert ist. Die Steuerung schlägt fehl, wenn das private ECR-Repository nicht für Scan on Push oder kontinuierliches Scannen konfiguriert ist.

Das Scannen von ECR-Bildern hilft bei der Identifizierung von Softwareschwachstellen in Ihren Container-Images. Die Konfiguration von Bildscans in ECR-Repositorys bietet eine zusätzliche Überprüfungsebene für die Integrität und Sicherheit der gespeicherten Bilder.

Abhilfe

Informationen zum Konfigurieren von Bildscans für ein ECR-Repository finden Sie unter [Scannen von Bildern](#) im Amazon Elastic Container Registry User Guide.

[ECR.2] Bei privaten ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-8 (1)

Kategorie: Identifizieren > Inventar > Etikettieren

Schweregrad: Mittel

Art der Ressource: AWS::ECR::Repository

AWS Config -Regel: [ecr-private-tag-immutability-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob in einem privaten ECR-Repository die Tag-Unveränderlichkeit aktiviert ist. Diese Kontrolle schlägt fehl, wenn in einem privaten ECR-Repository die Tag-

Unveränderlichkeit deaktiviert ist. Diese Regel gilt, wenn die Tag-Unveränderlichkeit aktiviert ist und den Wert hat. IMMUTABLE

Amazon ECR Tag Immutability ermöglicht es Kunden, sich auf die beschreibenden Tags eines Bildes als zuverlässigen Mechanismus zur Nachverfolgung und eindeutigen Identifizierung von Bildern zu verlassen. Ein unveränderliches Tag ist statisch, was bedeutet, dass sich jedes Tag auf ein eindeutiges Bild bezieht. Dies verbessert die Zuverlässigkeit und Skalierbarkeit, da die Verwendung eines statischen Tags immer dazu führt, dass dasselbe Image bereitgestellt wird. Wenn sie konfiguriert ist, verhindert die Unveränderlichkeit von Tags, dass die Tags überschrieben werden, wodurch die Angriffsfläche reduziert wird.

Abhilfe

Informationen zum Erstellen eines Repositorys mit konfigurierten unveränderlichen Tags oder zum Aktualisieren der Image-Tag-Mutabilitätseinstellungen für ein vorhandenes Repository finden Sie unter [Image-Tag-Mutability](#) im Amazon Elastic Container Registry User Guide.

[ECR.3] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2)

Kategorie: Identifizieren > Ressourcenkonfiguration

Schweregrad: Mittel

Art der Ressource: AWS::ECR::Repository

AWS Config -Regel: [ecr-private-lifecycle-policy-configured](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob für ein Amazon ECR-Repository mindestens eine Lebenszyklusrichtlinie konfiguriert ist. Diese Kontrolle schlägt fehl, wenn für ein ECR-Repository keine Lebenszyklusrichtlinien konfiguriert sind.

Mit Amazon ECR-Lebenszyklusrichtlinien können Sie das Lebenszyklusmanagement von Images in einem Repository festlegen. Durch die Konfiguration von Lebenszyklusrichtlinien können Sie die Bereinigung ungenutzter Images und das Verfallsdatum von Images je nach Alter oder

Anzahl automatisieren. Durch die Automatisierung dieser Aufgaben können Sie verhindern, dass versehentlich veraltete Bilder in Ihrem Repository verwendet werden.

Abhilfe

Informationen zur Konfiguration einer Lifecycle-Richtlinie finden Sie unter [Creating a Lifecycle Policy Preview](#) im Amazon Elastic Container Registry User Guide.

[ECR.4] Öffentliche ECR-Repositoryn sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::ECR::PublicRepository

AWS Config Regel: tagged-ecr-publicrepository (benutzerdefinierte Security Hub Hub-Regel)

Zeitplanytyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
requiredTagKeys	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein öffentliches Amazon ECR-Repository Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Kontrolle schlägt fehl, wenn das öffentliche Repository keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt

fehl, wenn das öffentliche Repository mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem öffentlichen ECR-Repository finden Sie unter [Tagging an ein öffentliches Amazon ECR-Repository](#) im Amazon Elastic Container Registry-Benutzerhandbuch.

[ECR.5] ECR-Repositorys sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys

Verwandte Anforderungen: NIST.800-53.r5 SC-1 2 (2), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8 (1), (10), (1), NIST.800-53.r5 SC-7 NIST.800-53.R5 NIST.800-53.r5 SC-2 SI-7 NIST.800-53.r5 CA-9 (6), NIST.800-53.R5 AU-9

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: `AWS::ECR::Repository`

AWS Config -Regel: [ecr-repository-cmk-encryption-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>kmsKeyArns</code>	Eine Liste von Amazon-Ressourcennamen (ARNs) AWS KMS keys , die in die Bewertung aufgenommen werden sollen. Das Steuerelement generiert einen FAILED Befund, wenn ein ECR-Repository nicht mit einem KMS-Schlüssel in der Liste verschlüsselt ist.	StringList (maximal 10 Elemente)	1—10 ARNs der vorhandenen KMS-Schlüssel. Beispiel: <code>arn:aws:kms:us-west-2:11112223333:key/1234abcd-12ab-34cd-56ef-1234567890ab</code>	Kein Standardwert

Diese Kontrolle prüft, ob ein Amazon ECR-Repository im Ruhezustand verschlüsselt ist und von einem Kunden verwaltet AWS KMS key wird. Die Kontrolle schlägt fehl, wenn das ECR-Repository nicht mit einem vom Kunden verwalteten KMS-Schlüssel verschlüsselt ist. Sie können optional eine Liste von KMS-Schlüsseln angeben, die das Steuerelement in die Bewertung einbeziehen soll.

Standardmäßig verschlüsselt Amazon ECR Repository-Daten mit Amazon S3 S3-verwalteten Schlüsseln (SSE-S3) unter Verwendung eines AES-256-Algorithmus. Für zusätzliche Kontrolle können Sie Amazon ECR so konfigurieren, dass die Daten stattdessen mit einem AWS KMS key (SSE-KMS oder DSSE-KMS) verschlüsselt werden. Der KMS-Schlüssel kann sein: ein Von AWS

verwalteter Schlüssel, den Amazon ECR für Sie erstellt und verwaltet und der den Alias `hataws/ecr`, oder ein vom Kunden verwalteter Schlüssel, den Sie in Ihrem AWS-Konto erstellen und verwalten. Mit einem vom Kunden verwalteten KMS-Schlüssel haben Sie die volle Kontrolle über den Schlüssel. Dazu gehören die Definition und Pflege der Schlüsselrichtlinie, die Verwaltung von Zuschüssen, die Rotation von kryptografischem Material, die Zuweisung von Tags, die Erstellung von Aliasnamen sowie die Aktivierung und Deaktivierung des Schlüssels.

Note

AWS KMS unterstützt den kontoübergreifenden Zugriff auf KMS-Schlüssel. Wenn ein ECR-Repository mit einem KMS-Schlüssel verschlüsselt ist, der einem anderen Konto gehört, führt dieses Steuerelement bei der Auswertung des Repositorys keine kontoübergreifenden Prüfungen durch. Die Kontrolle bewertet nicht, ob Amazon ECR auf den Schlüssel zugreifen und ihn verwenden kann, wenn kryptografische Operationen für das Repository ausgeführt werden.

Abhilfe

Sie können die Verschlüsselungseinstellungen für ein vorhandenes ECR-Repository nicht ändern. Sie können jedoch andere Verschlüsselungseinstellungen für ECR-Repositorys angeben, die Sie anschließend erstellen. Amazon ECR unterstützt die Verwendung verschiedener Verschlüsselungseinstellungen für einzelne Repositorys.

Weitere Informationen zu Verschlüsselungsoptionen für ECR-Repositorys finden Sie unter [Encryption at rest](#) im Amazon ECR-Benutzerhandbuch. Weitere Informationen zu „Customer Managed AWS KMS keys“ finden Sie [AWS KMS keys](#) im Developer Guide. AWS Key Management Service

Security Hub-Steuerelemente für Amazon ECS

Diese Security Hub Hub-Kontrollen bewerten den Service und die Ressourcen von Amazon Elastic Container Service (Amazon ECS). Die Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[ECS.1] Amazon ECS-Aufgabendefinitionen sollten sichere Netzwerkmodi und Benutzerdefinitionen enthalten

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Hoch

Art der Ressource: AWS::ECS::TaskDefinition

AWS Config -Regel: [ecs-task-definition-user-for-host-mode-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- SkipInactiveTaskDefinitions: true (nicht anpassbar)

Dieses Steuerelement prüft, ob eine aktive Amazon ECS-Aufgabendefinition mit Host-Netzwerkmodus `user` Container-Definitionen `privileged` hat. Die Steuerung schlägt bei Aufgabendefinitionen fehl, die Host-Netzwerkmodus- und Container-Definitionen `privileged=false`, leer und `user=root` oder leer haben.

Dieses Steuerelement bewertet nur die letzte aktive Revision einer Amazon ECS-Aufgabendefinition.

Mit dieser Steuerung soll sichergestellt werden, dass der Zugriff bewusst definiert wird, wenn Sie Aufgaben ausführen, die den Host-Netzwerkmodus verwenden. Wenn eine Aufgabendefinition über erhöhte Rechte verfügt, liegt das daran, dass Sie diese Konfiguration gewählt haben. Dieses Steuerelement sucht nach unerwarteter Rechteerweiterung, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist und Sie keine erhöhten Rechte wählen.

Abhilfe

Informationen zum Aktualisieren einer Aufgabendefinition finden Sie unter [Aktualisieren einer Aufgabendefinition](#) im Amazon Elastic Container Service Developer Guide.

Wenn Sie eine Aufgabendefinition aktualisieren, werden laufende Aufgaben, die mit der vorherigen Aufgabendefinition gestartet wurden, nicht aktualisiert. Um eine laufende Aufgabe zu aktualisieren, müssen Sie die Aufgabe mit der neuen Aufgabendefinition erneut bereitstellen.

[ECS.2] ECS-Diensten sollten nicht automatisch öffentliche IP-Adressen zugewiesen werden

Verwandte Anforderungen: NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7,

NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v4.0.1/1.4.4

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Hoch

Art der Ressource: AWS::ECS::Service

AWS Config Regel: `ecs-service-assign-public-ip-disabled` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Amazon ECS-Services so konfiguriert sind, dass sie automatisch öffentliche IP-Adressen zuweisen. Diese Steuerung schlägt fehl, wenn `AssignPublicIP` der Fall ist `ENABLED`. Diese Kontrolle `AssignPublicIP` ist erfolgreich, falls `jaDISABLED`.

Eine öffentliche IP-Adresse ist eine IP-Adresse, die über das Internet erreichbar ist. Wenn Sie Ihre Amazon ECS-Instances mit einer öffentlichen IP-Adresse starten, sind Ihre Amazon ECS-Instances über das Internet erreichbar. Amazon ECS-Services sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Container-Anwendungsserver ermöglichen kann.

Abhilfe

Zunächst müssen Sie eine Aufgabendefinition für Ihren Cluster erstellen, die den `awsvpc` Netzwerkmodus verwendet und `FARGATE` für spezifiziert. `requiresCompatibilities` Wählen Sie dann für Compute-Konfiguration die Optionen Starttyp und `FARGATE` aus. Schalten Sie abschließend für das Feld Netzwerk die Option Öffentliche IP aus, um die automatische Zuweisung öffentlicher IP-Adressen für Ihren Dienst zu deaktivieren.

[ECS.3] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Identifizieren > Ressourcenkonfiguration

Schweregrad: Hoch

Art der Ressource: `AWS::ECS::TaskDefinition`

AWS Config -Regel: [ecs-task-definition-pid-mode-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Amazon ECS-Aufgabendefinitionen so konfiguriert sind, dass sie den Prozess-Namespace eines Hosts gemeinsam mit seinen Containern verwenden. Die Steuerung schlägt fehl, wenn die Aufgabendefinition den Prozess-Namespace des Hosts gemeinsam mit den darauf laufenden Containern verwendet. Dieses Steuerelement bewertet nur die letzte aktive Revision einer Amazon ECS-Aufgabendefinition.

Ein Prozess-ID-Namespace (PID) sorgt für die Trennung zwischen Prozessen. Er verhindert, dass Systemprozesse sichtbar sind, und PIDs ermöglicht deren Wiederverwendung, einschließlich PID 1. Wenn der PID-Namespace des Hosts gemeinsam mit Containern genutzt wird, könnten Container alle Prozesse auf dem Hostsystem sehen. Dies verringert den Vorteil der Isolierung auf Prozessebene zwischen dem Host und den Containern. Diese Umstände könnten zu unberechtigtem Zugriff auf Prozesse auf dem Host selbst führen, einschließlich der Möglichkeit, diese zu manipulieren und zu beenden. Kunden sollten den Prozess-Namespace des Hosts nicht mit Containern teilen, die darauf laufen.

Abhilfe

Informationen zur Konfiguration der `pidMode` Aufgabendefinition finden Sie unter [Aufgabendefinitionsparameter](#) im Amazon Elastic Container Service Developer Guide.

[ECS.4] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6

Kategorie: Schützen > Sichere Zugriffsverwaltung > Zugriffsbeschränkungen für Root-Benutzer

Schweregrad: Hoch

Art der Ressource: `AWS::ECS::TaskDefinition`

AWS Config -Regel: [ecs-containers-nonprivileged](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der `privileged` Parameter in der Container-Definition von Amazon ECS-Aufgabendefinitionen auf `gesetzt` ist `true`. Die Steuerung schlägt fehl, wenn dieser Parameter gleich `ist` `true`. Dieses Steuerelement bewertet nur die letzte aktive Revision einer Amazon ECS-Aufgabendefinition.

Wir empfehlen, dass Sie erhöhte Rechte aus Ihren ECS-Aufgabendefinitionen entfernen. Wenn der Berechtigungsparameter lautet `true`, erhält der Container erhöhte Rechte auf der Host-Container-Instance (ähnlich wie dem Root-Benutzer).

Abhilfe

Informationen zur Konfiguration des `privileged` Parameters für eine Aufgabendefinition finden Sie unter [Erweiterte Container-Definitionsparameter](#) im Amazon Elastic Container Service Developer Guide.

[ECS.5] ECS-Container sollten auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1), (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Hoch

Art der Ressource: `AWS::ECS::TaskDefinition`

AWS Config -Regel: [ecs-containers-readonly-access](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon ECS-Container schreibgeschützten Zugriff auf sein Root-Dateisystem hat. Die Steuerung schlägt fehl `false`, wenn der `readonlyRootFilesystem`

Parameter auf gesetzt ist oder der Parameter in der Containerdefinition innerhalb der Aufgabendefinition nicht vorhanden ist. Dieses Steuerelement bewertet nur die letzte aktive Revision einer Amazon ECS-Aufgabendefinition.

Wenn der `readonlyRootFilesystem` Parameter `true` in einer Amazon ECS-Aufgabendefinition auf gesetzt ist, erhält der ECS-Container schreibgeschützten Zugriff auf sein Root-Dateisystem. Dadurch werden Sicherheitsangriffsvektoren reduziert, da das Root-Dateisystem der Container-Instance ohne explizite Volume-Mounts, die über Lese- und Schreibberechtigungen für Dateisystemordner und -verzeichnisse verfügen, nicht manipuliert oder darauf geschrieben werden kann. Die Aktivierung dieser Option entspricht auch dem Prinzip der geringsten Rechte.

Abhilfe

Um einem Amazon ECS-Container schreibgeschützten Zugriff auf sein Root-Dateisystem zu gewähren, fügen Sie den `readonlyRootFilesystem` Parameter zur Aufgabendefinition für den Container hinzu und setzen Sie den Wert für den Parameter auf `true`. Informationen zu Aufgabendefinitionsparametern und deren Hinzufügen zu einer Aufgabendefinition finden Sie unter [Amazon ECS-Aufgabendefinitionen](#) und [Aktualisieren einer Aufgabendefinition](#) im Amazon Elastic Container Service Developer Guide.

[ECS.8] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2, PCI DSS v4.0.1/8.6.2

Kategorie: Schützen > Sichere Entwicklung > Anmeldeinformationen sind nicht fest codiert

Schweregrad: Hoch

Art der Ressource: `AWS::ECS::TaskDefinition`

AWS Config -Regel: [ecs-no-environment-secrets](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: `secretKeys:AWS_ACCESS_KEY_ID,AWS_SECRET_ACCESS_KEY,ECS_ENGINE_AUTH_DATA` (nicht anpassbar)

Dieses Steuerelement prüft, ob der Schlüsselwert einer Variablen im `environment` Parameter von Containerdefinitionen `AWS_ACCESS_KEY_ID,AWS_SECRET_ACCESS_KEY`,

oder enthält ECS_ENGINE_AUTH_DATA. Dieses Steuerelement schlägt fehl, wenn eine einzelne Umgebungsvariable in einer Containerdefinition gleich AWS_ACCESS_KEY_ID, AWS_SECRET_ACCESS_KEY, oder ECS_ENGINE_AUTH_DATA ist. Diese Kontrolle deckt keine Umgebungsvariablen ab, die von anderen Standorten wie Amazon S3 weitergegeben werden. Dieses Steuerelement bewertet nur die letzte aktive Revision einer Amazon ECS-Aufgabendefinition.

AWS Systems Manager Parameter Store kann Ihnen helfen, die Sicherheitslage Ihres Unternehmens zu verbessern. Wir empfehlen, den Parameter Store zum Speichern von Geheimnissen und Anmeldeinformationen zu verwenden, anstatt sie direkt an Ihre Container-Instances zu übergeben oder sie fest in Ihren Code zu codieren.

Abhilfe

Informationen zum Erstellen von Parametern mit SSM finden Sie unter [Erstellen von Systems Manager Parameter-Parametern](#) im AWS Systems Manager Benutzerhandbuch. Weitere Informationen zum Erstellen einer Aufgabendefinition, die ein Geheimnis spezifiziert, finden Sie unter [Spezifizieren sensibler Daten mit dem Secrets Manager](#) im Amazon Elastic Container Service Developer Guide.

[ECS.9] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Hoch

Art der Ressource: AWS::ECS::TaskDefinition

AWS Config Regel: ecs-task-definition-log [Konfiguration](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für die letzte aktive Amazon ECS-Aufgabendefinition eine Protokollierungskonfiguration angegeben wurde. Die Steuerung schlägt fehl, wenn für die

Aufgabendefinition die `logConfiguration` Eigenschaft nicht definiert `logDriver` ist oder wenn der Wert für in mindestens einer Containerdefinition Null ist.

Die Protokollierung hilft Ihnen dabei, die Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon ECS aufrechtzuerhalten. Das Sammeln von Daten aus Aufgabendefinitionen bietet Transparenz, was Ihnen helfen kann, Prozesse zu debuggen und die Ursache von Fehlern zu finden. Wenn Sie eine Protokollierungslösung verwenden, die nicht in der ECS-Aufgabendefinition definiert werden muss (z. B. eine Protokollierungslösung eines Drittanbieters), können Sie diese Steuerung deaktivieren, nachdem Sie sichergestellt haben, dass Ihre Protokolle ordnungsgemäß erfasst und übermittelt wurden.

Abhilfe

Informationen zum Definieren einer Protokollkonfiguration für Ihre Amazon ECS-Aufgabendefinitionen finden Sie [unter Angeben einer Protokollkonfiguration in Ihrer Aufgabendefinition](#) im Amazon Elastic Container Service Developer Guide.

[ECS.10] Die ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen

Verwandte Anforderungen: NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), NIST.800-53.R5 SI-2 (5), PCI DSS v4.0.1/6.3.3

Kategorie: Identifizieren > Sicherheitslücken-, Patch- und Versionsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::ECS::Service`

AWS Config -Regel: [ecs-fargate-latest-platform-version](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `latestLinuxVersion`: 1.4.0(nicht anpassbar)
- `latestWindowsVersion`: 1.0.0(nicht anpassbar)

Dieses Steuerelement prüft, ob die Amazon ECS Fargate-Dienste die neueste Version der Fargate-Plattform ausführen. Diese Steuerung schlägt fehl, wenn die Plattformversion nicht die neueste ist.

AWS Fargate Plattformversionen beziehen sich auf eine spezifische Laufzeitumgebung für die Fargate-Task-Infrastruktur, bei der es sich um eine Kombination aus Kernel- und Container-Laufzeitversionen handelt. Neue Plattformversionen werden veröffentlicht, wenn sich die Laufzeitumgebung weiterentwickelt. Beispielsweise kann eine neue Version für Kernel- oder Betriebssystemupdates, neue Funktionen, Bugfixes oder Sicherheitsupdates veröffentlicht werden. Sicherheits-Updates und -Patches für Ihre -Fargate-Aufgaben werden automatisch bereitgestellt. Wenn ein Sicherheitsproblem gefunden wird, das sich auf eine Plattformversion auswirkt, wird die AWS Plattformversion gepatcht.

Abhilfe

Informationen zum Aktualisieren eines vorhandenen Service, einschließlich seiner Plattformversion, finden Sie unter [Aktualisieren eines Service](#) im Amazon Elastic Container Service Developer Guide.

[ECS.12] ECS-Cluster sollten Container Insights verwenden

Verwandte Anforderungen: NIST.800-53.R5 NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7 SI-2

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS::ECS::Cluster

AWS Config -Regel: [ecs-container-insights-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ECS-Cluster Container Insights verwenden. Diese Steuerung schlägt fehl, wenn Container Insights nicht für einen Cluster eingerichtet ist.

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon ECS-Clustern. Verwenden Sie CloudWatch Container Insights, um Metriken und Protokolle aus Ihren containerisierten Anwendungen und Microservices zu sammeln, zu aggregieren und zusammenzufassen. CloudWatch sammelt automatisch Metriken für viele Ressourcen wie CPU, Arbeitsspeicher, Festplatte und Netzwerk. Container Insights bietet auch Diagnoseinformationen, wie z. B. Fehler beim Container-Neustart, damit Sie Probleme schnell

aufdecken und beheben können. Sie können auch CloudWatch Alarme für Metriken einrichten, die Container Insights sammelt.

Abhilfe

Informationen zur Verwendung von Container Insights finden Sie unter [Service aktualisieren](#) im CloudWatch Amazon-Benutzerhandbuch.

[ECS.13] ECS-Services sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::ECS::Service`

AWS Config Regel: `tagged-ecs-service` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon ECS-Service Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind `requiredTagKeys`. Die Steuerung schlägt fehl, wenn der Service keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft

das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Dienst mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem ECS-Service finden Sie unter [Tagging your Amazon ECS-Ressourcen](#) im Amazon Elastic Container Service Developer Guide.

[ECS.14] ECS-Cluster sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::ECS::Cluster`

AWS Config Regel: `tagged-ecs-cluster` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon ECS-Cluster Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind `requiredTagKeys`. Die Steuerung schlägt fehl, wenn der Cluster keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Cluster mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `aws:` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem ECS-Cluster finden Sie unter [Tagging your Amazon ECS-Ressourcen](#) im Amazon Elastic Container Service Developer Guide.

[ECS.15] ECS-Aufgabendefinitionen sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Kennzeichnung

Schweregrad: Niedrig

Art der Ressource: `AWS::ECS::TaskDefinition`

AWS Config Regel: `tagged-ecs-taskdefinition` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon ECS-Aufgabendefinition Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind `requiredTagKeys`. Das Steuerelement schlägt fehl, wenn die Aufgabendefinition keine Tagschlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Aufgabendefinition mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` , werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer ECS-Aufgabendefinition finden Sie unter [Tagging your Amazon ECS-Ressourcen](#) im Amazon Elastic Container Service Developer Guide.

[ECS.16] ECS-Aufgabensätze sollten öffentliche IP-Adressen nicht automatisch zuweisen

Verwandte Anforderungen: PCI DSS v4.0.1/1.4.4

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Hoch

Art der Ressource: AWS::ECS::TaskSet

AWS Config Regel: `ecs-taskset-assign-public-ip-disabled` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon ECS-Task-Set so konfiguriert ist, dass öffentliche IP-Adressen automatisch zugewiesen werden. Die Steuerung schlägt fehl, wenn sie auf gesetzt `AssignPublicIP` ist `ENABLED`.

Eine öffentliche IP-Adresse ist über das Internet erreichbar. Wenn Sie Ihr Task-Set mit einer öffentlichen IP-Adresse konfigurieren, können die mit dem Task-Set verknüpften Ressourcen über das Internet erreicht werden. ECS-Aufgabensätze sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Container-Anwendungsserver ermöglichen kann.

Abhilfe

Informationen zum Aktualisieren eines ECS-Aufgabensatzes, sodass er keine öffentliche IP-Adresse verwendet, finden Sie unter [Aktualisieren einer Amazon ECS-Aufgabendefinition mithilfe der Konsole](#) im Amazon Elastic Container Service Developer Guide.

[ECS.17] ECS-Aufgabendefinitionen sollten nicht den Host-Netzwerkmodus verwenden

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: AWS::ECS::TaskDefinition

AWS Config -Regel: [ecs-task-definition-network-mode-not-host](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die letzte aktive Revision einer Amazon ECS-Aufgabendefinition den `host` Netzwerkmodus verwendet. Die Steuerung schlägt fehl, wenn die letzte aktive Revision der ECS-Aufgabendefinition den `host` Netzwerkmodus verwendet.

Bei Verwendung des `host` Netzwerkmodus ist das Netzwerk eines Amazon ECS-Containers direkt an den zugrunde liegenden Host gebunden, auf dem der Container ausgeführt wird. Folglich ermöglicht dieser Modus Containern, sich mit privaten Loopback-Netzwerkdiensten auf dem Host zu verbinden und sich als der Host auszugeben. Weitere wichtige Nachteile bestehen darin, dass es im `host` Netzwerkmodus keine Möglichkeit gibt, einen Container-Port neu zuzuordnen, und dass Sie nicht mehr als eine einzelne Instanziierung einer Aufgabe auf jedem Host ausführen können.

Abhilfe

Informationen zu Netzwerkmodi und Optionen für Amazon ECS-Aufgaben, die auf EC2 Amazon-Instances gehostet werden, finden Sie unter [Netzwerkoptionen für Amazon ECS-Aufgaben für den EC2 Starttyp](#) im Amazon Elastic Container Service Developer Guide. Informationen zum Erstellen einer neuen Version einer Aufgabendefinition und zum Angeben eines anderen Netzwerkmodus finden Sie in diesem Handbuch unter [Aktualisieren einer Amazon ECS-Aufgabendefinition](#).

Wenn die Amazon ECS-Aufgabendefinition von erstellt wurde AWS Batch, finden Sie unter [Netzwerkmodi für AWS Batch Jobs](#) Informationen zu Netzwerkmodi und zur typischen Verwendung von AWS Batch Auftragstypen sowie zur Auswahl einer sicheren Option.

Security Hub-Steuerelemente für Amazon EFS

Diese Security Hub Hub-Kontrollen bewerten den Service und die Ressourcen des Amazon Elastic File System (Amazon EFS).

Diese Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[EFS.1] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/2.4.1, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 (1), (10), NIST.800-53.r5 NIST.800-53.r5 SC-2 SI-7 (6) NIST.800-53.r5 SC-7

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: AWS::EFS::FileSystem

AWS Config -Regel: [efs-encrypted-check](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob Amazon Elastic File System so konfiguriert ist, dass es die Dateidaten verschlüsselt mit AWS KMS. Die Prüfung schlägt in den folgenden Fällen fehl.

- Encryptedist false in der [DescribeFileSystems](#)Antwort auf eingestellt.
- Der KmsKeyId-Schlüssel in der [DescribeFileSystems](#)-Antwort stimmt nicht mit dem KmsKeyId-Parameter für [efs-encrypted-check](#) überein.

Beachten Sie, dass dieses Steuerelement den KmsKeyId-Parameter nicht für [efs-encrypted-check](#) verwendet. Es überprüft nur den Wert von Encrypted.

Für eine zusätzliche Sicherheitsebene für Ihre sensiblen Daten in Amazon EFS sollten Sie verschlüsselte Dateisysteme erstellen. Amazon EFS unterstützt die Verschlüsselung von Dateisystemen im Ruhezustand. Sie können die Verschlüsselung von Daten im Ruhezustand aktivieren, wenn Sie ein Amazon EFS-Dateisystem erstellen. Weitere Informationen zur Amazon EFS-Verschlüsselung finden Sie unter [Datenverschlüsselung in Amazon EFS](#) im Amazon Elastic File System-Benutzerhandbuch.

Abhilfe

Einzelheiten zur Verschlüsselung eines neuen Amazon EFS-Dateisystems finden Sie unter [Verschlüsseln ruhender Daten im](#) Amazon Elastic File System-Benutzerhandbuch.

[EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-12, NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Resilienz > Backup

Schweregrad: Mittel

Art der Ressource: AWS::EFS::FileSystem

AWS Config -Regel: [efs-in-backup-plan](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob Amazon Elastic File System (Amazon EFS) -Dateisysteme zu den Sicherungsplänen in hinzugefügt wurden AWS Backup. Die Kontrolle schlägt fehl, wenn Amazon EFS-Dateisysteme nicht in den Backup-Plänen enthalten sind.

Die Einbeziehung von EFS-Dateisystemen in die Backup-Pläne hilft Ihnen, Ihre Daten vor Löschung und Datenverlust zu schützen.

Abhilfe

Informationen zum Aktivieren automatischer Backups für ein vorhandenes Amazon EFS-Dateisystem finden Sie unter [Erste Schritte 4: Automatische Amazon EFS-Backups erstellen](#) im AWS Backup Entwicklerhandbuch.

[EFS.3] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen

Verwandte Anforderungen: NIST.800-53.r5 AC-6 (10)

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: AWS::EFS::AccessPoint

AWS Config -Regel: [efs-access-point-enforce-root-directory](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob Amazon EFS-Zugriffspunkte so konfiguriert sind, dass sie ein Stammverzeichnis erzwingen. Die Steuerung schlägt fehl, wenn der Path Wert von auf / (das Standard-Stammverzeichnis des Dateisystems) gesetzt ist.

Wenn Sie ein Stammverzeichnis erzwingen, verwendet der NFS-Client, der den Zugriffspunkt verwendet, das auf dem Zugriffspunkt konfigurierte Stammverzeichnis anstelle des

Stammverzeichnis des Dateisystems. Durch die Festlegung eines Stammverzeichnisses für einen Access Point wird der Datenzugriff eingeschränkt, da sichergestellt wird, dass Benutzer des Access Points nur auf Dateien des angegebenen Unterverzeichnisses zugreifen können.

Abhilfe

Anweisungen zum Erzwingen eines Stammverzeichnisses für einen Amazon EFS-Zugriffspunkt finden Sie unter [Erzwingen eines Stammverzeichnisses mit einem Zugriffspunkt](#) im Amazon Elastic File System-Benutzerhandbuch.

[EFS.4] EFS-Zugangspunkte sollten eine Benutzeridentität erzwingen

Verwandte Anforderungen: NIST.800-53.r5 AC-6 (2), PCI DSS v4.0.1/7.3.1

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: AWS::EFS::AccessPoint

AWS Config -Regel: [efs-access-point-enforce-user-identity](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob Amazon EFS Access Points so konfiguriert sind, dass sie eine Benutzeridentität erzwingen. Diese Steuerung schlägt fehl, wenn beim Erstellen des EFS-Zugriffspunkts keine POSIX-Benutzeridentität definiert wurde.

Amazon-EFS-Zugangspunkte sind anwendungsspezifische Einstiegspunkte in ein EFS-Dateisystem, die das Verwalten des Anwendungszugriffs auf freigegebene Datensätze erleichtern. Zugriffspunkte können eine Benutzeridentität, einschließlich der POSIX-Gruppen des Benutzers, für alle Dateisystemanforderungen erzwingen, die über den Zugriffspunkt erfolgen. Zugriffspunkte können auch ein anderes Stammverzeichnis für das Dateisystem erzwingen, so dass Clients nur auf Daten im angegebenen Verzeichnis oder in seinen Unterverzeichnissen zugreifen können.

Abhilfe

Informationen zur Durchsetzung einer Benutzeridentität für einen Amazon EFS Access Point finden Sie unter [Durchsetzung einer Benutzeridentität mithilfe eines Access Points](#) im Amazon Elastic File System-Benutzerhandbuch.

[EFS.5] EFS-Zugangspunkte sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EFS::AccessPoint`

AWS Config Regel: `tagged-efs-accesspoint` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon EFS-Zugriffspunkt über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter definiert sind `requiredTagKeys`. Die Kontrolle schlägt fehl, wenn der Access Point keine Tag-Schlüssel hat oder wenn er nicht über alle im Parameter angegebenen Schlüssel verfügt `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft die Steuerung nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Access Point mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern

verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EFS-Zugangspunkt finden Sie unter [Tagging Amazon EFS-Ressourcen](#) im Amazon Elastic File System-Benutzerhandbuch.

[EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Mittel

Art der Ressource: `AWS::EFS::FileSystem`

AWS Config -Regel: [efs-mount-target-public-accessible](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon EFS-Mount-Ziel einem privaten Subnetz zugeordnet ist. Die Steuerung schlägt fehl, wenn das Mount-Ziel einem öffentlichen Subnetz zugeordnet ist.

Standardmäßig ist ein Dateisystem nur von der Virtual Private Cloud (VPC) aus zugänglich, in der Sie es erstellt haben. Wir empfehlen, EFS-Mount-Ziele in privaten Subnetzen zu erstellen, auf die nicht

über das Internet zugegriffen werden kann. Dadurch wird sichergestellt, dass Ihr Dateisystem nur autorisierten Benutzern zugänglich ist und nicht für unbefugten Zugriff oder Angriffe anfällig ist.

Abhilfe

Sie können die Zuordnung zwischen einem EFS-Mount-Ziel und einem Subnetz nicht ändern, nachdem Sie das Mount-Ziel erstellt haben. Um ein vorhandenes Mount-Ziel einem anderen Subnetz zuzuordnen, müssen Sie ein neues Mount-Ziel in einem privaten Subnetz erstellen und dann das alte Mount-Ziel entfernen. Informationen zur Verwaltung von Mount-Zielen finden Sie unter [Erstellen und Verwalten von Mount-Zielen und Sicherheitsgruppen](#) im Amazon Elastic File System-Benutzerhandbuch.

[EFS.7] Bei EFS-Dateisystemen sollten automatische Backups aktiviert sein

Schweregrad: Mittel

Ressourcentyp: AWS::EFS::FileSystem

AWS Config -Regel: [efs-automatic-backups-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für ein Amazon EFS-Dateisystem automatische Backups aktiviert sind. Diese Steuerung schlägt fehl, wenn für das EFS-Dateisystem keine automatischen Backups aktiviert sind.

Eine Datensicherung ist eine Kopie Ihrer System-, Konfiguration- oder Anwendungsdaten, die getrennt vom Original gespeichert wird. Durch die Aktivierung regelmäßiger Backups können Sie wertvolle Daten vor unvorhergesehenen Ereignissen wie Systemausfällen, Cyberangriffen oder versehentlichem Löschen schützen. Eine robuste Backup-Strategie ermöglicht auch eine schnellere Wiederherstellung, einen unterbrechungsfreien Betrieb und sorgt für mehr Sicherheit angesichts potenzieller Datenverluste.

Abhilfe

Informationen AWS Backup zur Verwendung von EFS-Dateisystemen finden Sie unter [Sicherung von EFS-Dateisystemen](#) im Amazon Elastic File System-Benutzerhandbuch

[EFS.8] EFS-Dateisysteme sollten im Ruhezustand verschlüsselt werden

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: AWS::EFS::FileSystem

AWS Config -Regel: [efs-file-system-ct-encrypted](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon EFS-Dateisystem Daten mit AWS Key Management Service (AWS KMS) verschlüsselt. Die Steuerung schlägt fehl, wenn ein Dateisystem nicht verschlüsselt ist.

Daten im Ruhezustand beziehen sich auf Daten, die für einen beliebigen Zeitraum in einem persistenten, nichtflüchtigen Speicher gespeichert werden. Durch die Verschlüsselung ruhender Daten können Sie deren Vertraulichkeit schützen, wodurch das Risiko verringert wird, dass ein nicht autorisierter Benutzer darauf zugreifen kann.

Abhilfe

Informationen zum Aktivieren der Verschlüsselung im Ruhezustand für ein neues EFS-Dateisystem finden Sie unter [Verschlüsseln von Daten im Ruhezustand](#) im Amazon Elastic File System-Benutzerhandbuch.

Security Hub-Steuerelemente für Amazon EKS

Diese Security Hub Hub-Kontrollen bewerten den Service und die Ressourcen von Amazon Elastic Kubernetes Service (Amazon EKS). Die Steuerelemente sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[EKS.1] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v4.0.1/1.4.4

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Hoch

Art der Ressource: `AWS::EKS::Cluster`

AWS Config -Regel: [eks-endpoint-no-public-access](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon EKS-Cluster-Endpoint öffentlich zugänglich ist. Die Kontrolle schlägt fehl, wenn ein EKS-Cluster über einen öffentlich zugänglichen Endpoint verfügt.

Wenn Sie einen neuen Cluster erstellen, erstellt Amazon EKS einen Endpoint für den verwalteten Kubernetes-API-Server, den Sie für die Kommunikation mit Ihrem Cluster verwenden. Standardmäßig ist dieser API-Server-Endpoint öffentlich im Internet verfügbar. Der Zugriff auf den API-Server wird durch eine Kombination aus AWS Identity and Access Management (IAM) und nativer Kubernetes-Rollenbasierter Zugriffskontrolle (RBAC) gesichert. Indem Sie den öffentlichen Zugriff auf den Endpoint unterbinden, können Sie verhindern, dass Ihr Cluster unbeabsichtigt gefährdet ist und Sie darauf zugreifen können.

Abhilfe

Informationen zum Ändern des Endpointzugriffs für einen vorhandenen EKS-Cluster finden Sie unter [Ändern des Cluster-Endpointzugriffs](#) im Amazon EKS-Benutzerhandbuch. Sie können den Endpointzugriff für einen neuen EKS-Cluster einrichten, wenn Sie ihn erstellen. Anweisungen zum Erstellen eines neuen Amazon EKS-Clusters finden Sie unter [Erstellen eines Amazon EKS-Clusters](#) im Amazon EKS-Benutzerhandbuch.

[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), NIST.800-53.R5 SI-2 (5), PCI DSS v4.0.1/12.3.4

Kategorie: Identifizieren > Sicherheitslücken-, Patch- und Versionsverwaltung

Schweregrad: Hoch

Art der Ressource: `AWS::EKS::Cluster`

AWS Config -Regel: [eks-cluster-supported-version](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `oldestVersionSupported`: 1.31 (nicht anpassbar)

Dieses Steuerelement prüft, ob ein Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster auf einer unterstützten Kubernetes-Version ausgeführt wird. Die Steuerung schlägt fehl, wenn der EKS-Cluster auf einer nicht unterstützten Version ausgeführt wird.

Wenn Ihre Anwendung keine bestimmte Version von Kubernetes benötigt, empfehlen wir Ihnen, die neueste verfügbare Kubernetes-Version zu verwenden, die von EKS für Ihre Cluster unterstützt wird. Weitere Informationen finden Sie im [Amazon EKS Kubernetes-Veröffentlichungskalender](#) und im Amazon [EKS-Benutzerhandbuch im Überblick über den Lebenszyklus der Kubernetes-Version auf Amazon EKS](#).

Abhilfe

Informationen zum Aktualisieren eines EKS-Clusters finden Sie unter [Aktualisieren eines vorhandenen Clusters auf eine neue Kubernetes-Version](#) im Amazon EKS-Benutzerhandbuch.

[EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden

Verwandte Anforderungen: NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-1 2, NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, PCI DSS v4.0.1/8.3.2

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: `AWS::EKS::Cluster`

AWS Config -Regel: [eks-cluster-secrets-encrypted](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon EKS-Cluster verschlüsselte Kubernetes-Geheimnisse verwendet. Die Steuerung schlägt fehl, wenn die Kubernetes-Geheimnisse des Clusters nicht verschlüsselt sind.

Wenn Sie Geheimnisse verschlüsseln, können Sie AWS Key Management Service (AWS KMS) -Schlüssel verwenden, um die in etcd für Ihren Cluster gespeicherten Kubernetes-

Geheimnisse mit Umschlägen zu verschlüsseln. Diese Verschlüsselung erfolgt zusätzlich zur EBS-Volumenverschlüsselung, die standardmäßig für alle Daten (einschließlich Secrets) aktiviert ist, die in etcd als Teil eines EKS-Clusters gespeichert sind. Durch die Verschlüsselung von Geheimnissen für Ihren EKS-Cluster können Sie eine umfassende Verteidigungsstrategie für Kubernetes-Anwendungen implementieren, indem Sie Kubernetes-Geheimnisse mit einem KMS-Schlüssel verschlüsseln, den Sie definieren und verwalten.

Abhilfe

Informationen zum Aktivieren der Geheimverschlüsselung auf einem EKS-Cluster finden Sie unter [Enabling Secret Encryption on a existing cluster](#) im Amazon EKS-Benutzerhandbuch.

[EKS.6] EKS-Cluster sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EKS::Cluster`

AWS Config Regel: `tagged-eks-cluster` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon EKS-Cluster Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind `requiredTagKeys`. Die Steuerung schlägt fehl, wenn der

Cluster keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Cluster mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `aws:*` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der Allgemeinen AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EKS-Cluster finden Sie unter [Taggen Ihrer Amazon EKS-Ressourcen](#) im Amazon EKS-Benutzerhandbuch.

[EKS.7] Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EKS::IdentityProviderConfig`

AWS Config Regel: `tagged-eks-identityproviderconfig` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon EKS-Identitätsanbieter-Konfiguration Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind `requiredTagKeys`. Die Steuerung schlägt fehl, wenn die Konfiguration keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Konfiguration mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien

für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu Konfigurationen eines EKS-Identitätsanbieters finden Sie unter [Taggen Ihrer Amazon EKS-Ressourcen](#) im Amazon EKS-Benutzerhandbuch.

[EKS.8] Bei EKS-Clustern sollte die Auditprotokollierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (12), (4), NIST.800-53.r5 AC-2 (26), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-9(7), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.R5 SI-4, NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8), PCI DSS v4.0.1/10.2.1

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Ressourcentyp: AWS::EKS::Cluster

AWS Config -Regel: [eks-cluster-log-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- logTypes: audit(nicht anpassbar)

Dieses Steuerelement prüft, ob für einen Amazon EKS-Cluster die Auditprotokollierung aktiviert ist. Die Kontrolle schlägt fehl, wenn die Audit-Protokollierung für den Cluster nicht aktiviert ist.

 Note

Dieses Steuerelement überprüft nicht, ob die Amazon EKS-Auditprotokollierung über Amazon Security Lake für aktiviert ist AWS-Konto.

Die EKS-Protokollierung auf der Kontrollebene stellt Prüf- und Diagnoseprotokolle direkt von der EKS-Steuerebene zu Amazon CloudWatch Logs in Ihrem Konto bereit. Sie können die Protokolltypen auswählen, die Sie benötigen, und die Protokolle werden als Protokollstreams an eine Gruppe für jeden EKS-Cluster gesendet CloudWatch. Die Protokollierung bietet Einblick in den Zugriff und die Leistung von EKS-Clustern. Indem Sie die Protokolle der EKS-Kontrollebene für Ihre EKS-Cluster an CloudWatch Logs senden, können Sie Vorgänge zu Prüf- und Diagnosezwecken an einem zentralen Ort aufzeichnen.

Abhilfe

Informationen zum Aktivieren von Audit-Logs für Ihren EKS-Cluster finden Sie unter [Aktivieren und Deaktivieren von Control Plane-Protokollen](#) im Amazon EKS-Benutzerhandbuch.

Security Hub-Steuerungen für ElastiCache

Diese AWS Security Hub Kontrollen bewerten den ElastiCache Service und die Ressourcen von Amazon.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

Bei [ElastiCache.1] ElastiCache (Redis OSS) -Clustern sollten automatische Backups aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-12, NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Backups aktiviert

Schweregrad: Hoch

Ressourcentyp:AWS::ElastiCache::CacheCluster, AWS:ElastiCache:ReplicationGroup

AWS Config -Regel: [elasticache-redis-cluster-automatic-backup-check](#)

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
snapshotRetentionPeriod	Minimale Aufbewahrungsdauer für Snapshots in Tagen	Ganzzahl	1 auf 35	1

Diese Kontrolle bewertet, ob für einen Amazon ElastiCache (Redis OSS) -Cluster automatische Backups geplant sind. Die Steuerung schlägt fehl, wenn der SnapshotRetentionLimit für den Redis-Cluster angegebene Zeitraum kürzer als der angegebene Zeitraum ist. Sofern Sie keinen benutzerdefinierten Parameterwert für die Aufbewahrungsdauer von Snapshots angeben, verwendet Security Hub einen Standardwert von 1 Tag.

Amazon ElastiCache (Redis OSS) -Cluster können ihre Daten sichern. Sie können die Sicherung zur Wiederherstellung eines Clusters oder als Ausgangspunkt für einen neuen Cluster verwenden. Eine Sicherung besteht aus den Metadaten des Clusters zusammen mit allen Daten im Cluster. Alle Sicherungen werden in Amazon Simple Storage Service (Amazon S3) geschrieben, der einen dauerhaften Speicher bereitstellt. Sie können Ihre Daten wiederherstellen, indem Sie einen neuen Redis-Cluster erstellen und ihn mit Daten aus einem Backup füllen. Sie können Backups mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) und der ElastiCache API verwalten.

Abhilfe

Informationen zum Planen automatischer Backups auf einem ElastiCache (Redis OSS) -Cluster finden Sie unter [Automatische Backups planen](#) im ElastiCache Amazon-Benutzerhandbuch.

[ElastiCache.2] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), NIST.800-53.R5 SI-2 (5) PCI DSS v4.0.1/6.3.3

Kategorie: Identifizieren > Sicherheitslücken-, Patch- und Versionsverwaltung

Schweregrad: Hoch

Art der Ressource: AWS::ElastiCache::CacheCluster

AWS Config -Regel: [elasticache-auto-minor-version-upgrade-check](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle bewertet, ob Amazon ElastiCache automatisch kleinere Versions-Upgrades auf einen Cache-Cluster anwendet. Die Kontrolle schlägt fehl, wenn auf den Cache-Cluster keine automatischen Upgrades für Nebenversionen angewendet werden.

 Note

Diese Steuerung gilt nicht für ElastiCache Memcached-Cluster.

Das automatische Upgrade von Nebenversionen ist eine Funktion, die Sie in Amazon aktivieren können ElastiCache , um Ihre Cache-Cluster automatisch zu aktualisieren, wenn eine neue kleinere Cache-Engine-Version verfügbar ist. Diese Upgrades können Sicherheitspatches und Bugfixes beinhalten. Die up-to-date Beibehaltung der Patch-Installation ist ein wichtiger Schritt zur Sicherung der Systeme.

Abhilfe

Informationen zum automatischen Anwenden kleinerer Versions-Upgrades auf einen vorhandenen ElastiCache Cache-Cluster finden Sie unter [Versionsverwaltung für ElastiCache](#) im ElastiCache Amazon-Benutzerhandbuch.

[ElastiCache.3] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: AWS::ElastiCache::ReplicationGroup

AWS Config -Regel: [elasticache-repl-grp-auto-failover-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob für eine ElastiCache Replikationsgruppe das automatische Failover aktiviert ist. Die Steuerung schlägt fehl, wenn der automatische Failover für eine Replikationsgruppe nicht aktiviert ist.

Wenn der automatische Failover für eine Replikationsgruppe aktiviert ist, erfolgt für die Rolle des Primärknotens automatisch ein Failover auf eine der Read Replicas. Dieses Failover und die Replikatheraufstufung stellen sicher, dass Sie nach Abschluss der Heraufstufung wieder auf den neuen Primärserver schreiben können, wodurch die Gesamtausfallzeit im Falle eines Fehlers reduziert wird.

Abhilfe

Informationen zum Aktivieren des automatischen Failovers für eine bestehende ElastiCache Replikationsgruppe finden Sie unter [Modifizieren eines ElastiCache Clusters](#) im ElastiCache Amazon-Benutzerhandbuch. Wenn Sie die ElastiCache Konsole verwenden, setzen Sie Auto Failover auf aktiviert.

[ElastiCache.4] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: AWS::ElastiCache::ReplicationGroup

AWS Config -Regel: [elasticache-repl-grp-encrypted-at-rest](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob eine ElastiCache Replikationsgruppe im Ruhezustand verschlüsselt ist. Die Steuerung schlägt fehl, wenn die Replikationsgruppe im Ruhezustand nicht verschlüsselt ist.

Durch die Verschlüsselung von Daten im Ruhezustand wird das Risiko verringert, dass ein nicht authentifizierter Benutzer Zugriff auf Daten erhält, die auf der Festplatte gespeichert sind. ElastiCache (Redis OSS) Replikationsgruppen sollten im Ruhezustand verschlüsselt werden, um eine zusätzliche Sicherheitsebene zu gewährleisten.

Abhilfe

Informationen zur Konfiguration der Verschlüsselung im Ruhezustand für eine ElastiCache Replikationsgruppe finden Sie unter [Enabling at rest encryption](#) im ElastiCache Amazon-Benutzerhandbuch.

[ElastiCache.5] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 AC-1 7 (2), (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 NIST.800-53.r5 IA-5 (3), 3, 3, 3 (NIST.800-53.r5 SC-13), NIST.800-53.r5 SC-2 (4),, NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-7 (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.R5 SI-7 NIST.800-53.r5 SC-8 (6), PCI DSS v4.0.1/4.2.1

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: AWS::ElastiCache::ReplicationGroup

AWS Config -Regel: [elasticache-repl-grp-encrypted-in-transit](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob eine ElastiCache Replikationsgruppe während der Übertragung verschlüsselt ist. Die Steuerung schlägt fehl, wenn die Replikationsgruppe bei der Übertragung nicht verschlüsselt wird.

Durch die Verschlüsselung von Daten während der Übertragung wird das Risiko verringert, dass ein nicht autorisierter Benutzer den Netzwerkverkehr abhören kann. Wenn Sie die Verschlüsselung bei der Übertragung in einer ElastiCache Replikationsgruppe aktivieren, werden Ihre Daten immer dann

verschlüsselt, wenn sie von einem Ort an einen anderen übertragen werden, z. B. zwischen Knoten in Ihrem Cluster oder zwischen Ihrem Cluster und Ihrer Anwendung.

Abhilfe

Informationen zur Konfiguration der Verschlüsselung während der Übertragung für eine ElastiCache Replikationsgruppe finden Sie unter [Aktivieren der Verschlüsselung bei der Übertragung](#) im ElastiCache Amazon-Benutzerhandbuch.

[ElastiCache.6] Für Replikationsgruppen ElastiCache (Redis OSS) früherer Versionen sollte Redis OSS AUTH aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1), (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-3 (7), PCI DSS v4.0.1/8.3.1 NIST.800-53.r5 AC-6

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: AWS::ElastiCache::ReplicationGroup

AWS Config -Regel: [elasticache-repl-grp-redis-auth-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob für eine Replikationsgruppe ElastiCache (Redis OSS) Redis OSS AUTH aktiviert ist. Die Steuerung schlägt fehl, wenn die Redis OSS-Version der Replikationsgruppenknoten unter 6.0 liegt und AuthToken nicht verwendet wird.

Wenn Sie Redis-Authentifizierungstoken oder Passwörter verwenden, benötigt Redis ein Passwort, bevor Clients Befehle ausführen können, was die Datensicherheit verbessert. Für Redis 6.0 und spätere Versionen empfehlen wir die Verwendung von Role-Based Access Control (RBAC). Da RBAC für Redis-Versionen vor 6.0 nicht unterstützt wird, wertet dieses Steuerelement nur Versionen aus, die die RBAC-Funktion nicht verwenden können.

Abhilfe

Informationen zur Verwendung von Redis AUTH in einer ElastiCache (Redis OSS) Replikationsgruppe finden Sie unter [Ändern des AUTH-Tokens auf einem vorhandenen ElastiCache \(Redis OSS\) -Cluster](#) im Amazon-Benutzerhandbuch. ElastiCache

[ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden

Verwandte Anforderungen: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (5)

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Hoch

Art der Ressource: AWS::ElastiCache::CacheCluster

AWS Config -Regel: [elasticache-subnet-group-check](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein ElastiCache Cluster mit einer benutzerdefinierten Subnetzgruppe konfiguriert ist. Die Steuerung schlägt fehl, wenn CacheSubnetGroupName für einen ElastiCache Cluster der Wert default gilt.

Beim Starten eines ElastiCache Clusters wird eine Standard-Subnetzgruppe erstellt, falls noch keine vorhanden ist. Die Standardgruppe verwendet Subnetze aus der standardmäßigen Virtual Private Cloud (VPC). Wir empfehlen, benutzerdefinierte Subnetzgruppen zu verwenden, die die Subnetze, in denen sich der Cluster befindet, und die Netzwerke, die der Cluster von den Subnetzen erbt, restriktiver behandeln.

Abhilfe

Informationen zum Erstellen einer neuen Subnetzgruppe für einen ElastiCache Cluster finden Sie unter [Erstellen einer Subnetzgruppe](#) im ElastiCache Amazon-Benutzerhandbuch.

Security Hub-Steuerelemente für Elastic Beanstalk

Diese AWS Security Hub Kontrollen bewerten den AWS Elastic Beanstalk Service und die Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben

Verwandte Anforderungen: NIST.800-53.R5 NIST.800-53.r5 CA-7 SI-2

Kategorie: Erkennen > Erkennungsdienste > Anwendungsüberwachung

Schweregrad: Niedrig

Art der Ressource: AWS::ElasticBeanstalk::Environment

AWS Config -Regel: [beanstalk-enhanced-health-reporting-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die erweiterte Integritätsberichterstattung für Ihre AWS Elastic Beanstalk Umgebungen aktiviert ist.

Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen.

Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen. Der Elastic Beanstalk Health Agent, der in unterstützten Amazon Machine Images (AMIs) enthalten ist, wertet Logs und Metriken von Umgebungsinstanzen aus. EC2

Weitere Informationen finden Sie unter [Verbesserte Statusberichterstattung und Überwachung im AWS Elastic Beanstalk Entwicklerhandbuch](#).

Abhilfe

Anweisungen zur Aktivierung der erweiterten Zustandsberichterstattung finden Sie unter [Enabling enhanced Health Reporting using the Elastic Beanstalk Console](#) im AWS Elastic Beanstalk Developer Guide.

[ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), NIST.800-53.R5 SI-2 (5), PCI DSS v4.0.1/6.3.3

Kategorie: Identifizieren > Sicherheitslücken-, Patch- und Versionsverwaltung

Schweregrad: Hoch

Art der Ressource: AWS::ElasticBeanstalk::Environment

AWS Config -Regel: [elastic-beanstalk-managed-updates-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
UpdateLevel	Stufe des Versionsupdates	Enum	minor, patch	Kein Standardwert

Dieses Steuerelement prüft, ob verwaltete Plattformupdates für eine Elastic Beanstalk Beanstalk-Umgebung aktiviert sind. Die Steuerung schlägt fehl, wenn keine Updates für verwaltete Plattformen aktiviert sind. Standardmäßig ist die Steuerung erfolgreich, wenn irgendeine Art von Plattform-Update aktiviert ist. Optional können Sie einen benutzerdefinierten Parameterwert angeben, um eine bestimmte Aktualisierungsstufe zu erfordern.

Durch die Aktivierung verwalteter Plattformupdates wird sichergestellt, dass die neuesten verfügbaren Plattformkorrekturen, Updates und Funktionen für die Umgebung installiert werden. Die Aktualisierung der Patch-Installation ist ein wichtiger Schritt zur Sicherung der Systeme.

Abhilfe

Informationen zur Aktivierung verwalteter Plattformupdates finden Sie unter [So konfigurieren Sie verwaltete Plattformupdates unter Verwaltete Plattformupdates](#) im AWS Elastic Beanstalk Entwicklerhandbuch.

[ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch

Verwandte Anforderungen: PCI DSS v4.0.1/10.4.2

Kategorie: Identifizieren > Protokollierung

Schweregrad: Hoch

Art der Ressource: AWS::ElasticBeanstalk::Environment

AWS Config -Regel: [elastic-beanstalk-logs-to-cloudwatch](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
RetentionInDays	Anzahl der Tage, an denen Protokollereignisse vor Ablauf aufbewahrt werden sollen	Enum	1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365, 400, 545, 731, 1827, 3653	Kein Standardwert

Dieses Steuerelement prüft, ob eine Elastic Beanstalk Beanstalk-Umgebung so konfiguriert ist, dass sie Logs an CloudWatch Logs sendet. Die Steuerung schlägt fehl, wenn eine Elastic Beanstalk Beanstalk-Umgebung nicht so konfiguriert ist, dass sie Logs an CloudWatch Logs sendet. Optional können Sie einen benutzerdefinierten Wert für den RetentionInDays Parameter angeben, wenn Sie möchten, dass die Steuerung nur dann erfolgreich ist, wenn Logs für die angegebene Anzahl von Tagen vor Ablauf aufbewahrt werden.

CloudWatch hilft Ihnen dabei, verschiedene Messwerte für Ihre Anwendungen und Infrastrukturressourcen zu sammeln und zu überwachen. Sie können es auch verwenden CloudWatch , um Alarmaktionen auf der Grundlage bestimmter Metriken zu konfigurieren. Wir empfehlen die Integration von Elastic Beanstalk mit, CloudWatch um mehr Einblick in Ihre Elastic Beanstalk Beanstalk-Umgebung zu erhalten. Zu den Elastic Beanstalk Beanstalk-Protokollen gehören die Datei eb-activity.log, Zugriffsprotokolle vom Umgebungs-Nginx- oder Apache-Proxyserver sowie Protokolle, die für eine Umgebung spezifisch sind.

Abhilfe

Informationen zur Integration von Elastic Beanstalk mit CloudWatch Logs finden Sie im AWS Elastic Beanstalk Developer Guide unter [CloudWatch Instanzprotokolle streamen](#).

Security Hub-Steuerelemente für Elastic Load Balancing

Diese AWS Security Hub Kontrollen bewerten den Elastic Load Balancing Service und die Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[ELB.1] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden

Verwandte Anforderungen: PCI DSS v3.2.1/2.3, PCI DSS v3.2.1/4.1, NIST.800-53.r5 AC-1 7 (2), (1), 2 (3), 3 NIST.800-53.r5 AC-4, 3, 3 NIST.800-53.r5 IA-5 (3), (4),, NIST.800-53.r5 SC-1 (1), NIST.800-53.r5 SC-2 (NIST.800-53.r5 SC-12), NIST.800-53.r5 SC-2 NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-7 (6) NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config -Regel: [alb-http-to-https-redirection-check](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob die HTTP-zu-HTTPS-Umleitung auf allen HTTP-Listnern von Application Load Balancern konfiguriert ist. Die Steuerung schlägt fehl, wenn für einen der HTTP-Listener von Application Load Balancern keine HTTP-zu-HTTPS-Umleitung konfiguriert ist.

Bevor Sie Ihren Application Load Balancer verwenden können, müssen Sie einen oder mehrere Listener hinzufügen. Ein Listener ist ein Prozess, der das konfigurierte Protokoll und den Port verwendet, um nach Verbindungsanforderungen zu suchen. Listener unterstützen sowohl das HTTP- als auch das HTTPS-Protokoll. Sie können einen HTTPS-Listener verwenden, um die Arbeit der Verschlüsselung und Entschlüsselung auf Ihren Load Balancer auszulagern. Um die Verschlüsselung

während der Übertragung zu erzwingen, sollten Sie Umleitungsaktionen mit Application Load Balancers verwenden, um Client-HTTP-Anfragen an eine HTTPS-Anfrage an Port 443 umzuleiten.

Weitere Informationen finden Sie unter [Listener für Ihre Application Load Balancers](#) im Benutzerhandbuch für Application Load Balancers.

Abhilfe

Um HTTP-Anfragen an HTTPS umzuleiten, müssen Sie eine Application Load Balancer Listener-Regel hinzufügen oder eine bestehende Regel bearbeiten.

Anweisungen zum Hinzufügen einer neuen Regel finden Sie unter [Sie unter Regel hinzufügen](#) im Benutzerhandbuch für Application Load Balancers. Wählen Sie für Protocol: Port die Option HTTP und geben Sie dann ein **80**. Wählen Sie für Aktion hinzufügen die Option Umleiten zu die Option HTTPS aus, und geben Sie dann die Eingabetaste ein **443**.

Anweisungen zum Bearbeiten einer vorhandenen Regel finden Sie unter [Regel bearbeiten](#) im Benutzerhandbuch für Application Load Balancers. Wählen Sie für Protocol: Port die Option HTTP und geben Sie dann ein **80**. Wählen Sie für Aktion hinzufügen die Option Umleiten zu die Option HTTPS aus, und geben Sie dann die Eingabetaste ein **443**.

[ELB.2] Classic Load Balancer mit SSL/HTTPS Listnern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager

Verwandte Anforderungen: NIST.800-53.r5 AC-1 7 (2), (1) NIST.800-53.r5 AC-4, 2 NIST.800-53.r5 IA-5 (3), 3, 3, 3 (5), NIST.800-53.r5 SC-1 (4), (1), (NIST.800-53.r5 SC-12), NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-7 NIST.800-53.R5 SI-7 NIST.800-53.r5 SC-8 (6), NIST.800-53.r5 SC-8 NIST.800-171.r2 3.13.8 NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-8

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: AWS::ElasticLoadBalancing::LoadBalancer

AWS Config -Regel: [elb-acm-certificate-required](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der Classic Load Balancer von AWS Certificate Manager (ACM) bereitgestellte HTTPS/SSL Zertifikate verwendet. Die Steuerung schlägt fehl, wenn der mit dem HTTPS/SSL Listener konfigurierte Classic Load Balancer kein von ACM bereitgestelltes Zertifikat verwendet.

Um ein Zertifikat zu erstellen, können Sie entweder ACM oder ein Tool verwenden, das die SSL- und TLS-Protokolle unterstützt, z. B. OpenSSL. Security Hub empfiehlt, dass Sie ACM verwenden, um Zertifikate für Ihren Load Balancer zu erstellen oder zu importieren.

ACM ist in Classic Load Balancern integriert, sodass Sie das Zertifikat auf Ihrem Load Balancer bereitstellen können. Sie sollten diese Zertifikate auch automatisch erneuern.

Abhilfe

Informationen zum Zuordnen eines SSL/TLS ACM-Zertifikats zu einem Classic Load Balancer finden Sie im AWS Knowledge Center-Artikel [Wie kann ich ein SSL/TLS ACM-Zertifikat mit einem Classic-, Anwendungs- oder Network Load Balancer verknüpfen?](#)

[ELB.3] Classic Load Balancer Balancer-Listener sollten mit HTTPS- oder TLS-Terminierung konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 AC-1 7 (2), (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 NIST.800-53.r5 IA-5 (3), 3, 3 (NIST.800-53.r5 SC-13), NIST.800-53.r5 SC-2 3 (NIST.800-53.r5 SC-23), (4), NIST.800-53.r5 SC-7 (1), NIST.800-53.r5 SC-8 (2) NIST.800-53.r5 SC-8, NIST.800-53.R5 SI-7 NIST.800-53.r5 SC-8 (6), NIST.800-171.r2 3.13.8, NIST.800-171.r2 3.13.15, PCI DSS v4.0.1/4.2.1

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: AWS::ElasticLoadBalancing::LoadBalancer

AWS Config -Regel: [elb-tls-https-listeners-only](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Ihre Classic Load Balancer Balancer-Listener mit dem HTTPS- oder TLS-Protokoll für Front-End-Verbindungen (Client zu Load Balancer) konfiguriert sind. Die Steuerung

ist anwendbar, wenn ein Classic Load Balancer über Listener verfügt. Wenn für Ihren Classic Load Balancer kein Listener konfiguriert ist, meldet die Steuerung keine Ergebnisse.

Die Steuerung ist erfolgreich, wenn die Classic Load Balancer Balancer-Listener mit TLS oder HTTPS für Frontend-Verbindungen konfiguriert sind.

Die Steuerung schlägt fehl, wenn der Listener nicht mit TLS oder HTTPS für Frontend-Verbindungen konfiguriert ist.

Bevor Sie mit der Verwendung eines Load Balancers beginnen, müssen Sie einen oder mehrere Listener hinzufügen. Ein Listener ist ein Prozess, der das konfigurierte Protokoll und den Port verwendet, um nach Verbindungsanforderungen zu suchen. Listener können sowohl HTTP als auch Protokolle unterstützen. HTTPS/TLS Sie sollten immer einen HTTPS- oder TLS-Listener verwenden, damit der Load Balancer die Ver- und Entschlüsselung während der Übertragung übernimmt.

Abhilfe

Um dieses Problem zu beheben, aktualisieren Sie Ihre Listener so, dass sie das TLS- oder HTTPS-Protokoll verwenden.

Um alle nicht konformen Listener in Listener umzuwandeln TLS/HTTPS

1. Öffnen Sie die EC2 Amazon-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Load Balancers aus.
3. Wählen Sie Ihren Classic Load Balancer aus.
4. Wählen Sie auf der Registerkarte Listeners die Option Edit aus.
5. Ändern Sie für alle Listener, bei denen das Load Balancer-Protokoll nicht auf HTTPS oder SSL eingestellt ist, die Einstellung auf HTTPS oder SSL.
6. Wählen Sie für alle modifizierten Listener auf der Registerkarte Zertifikate die Option Standard ändern aus.
7. Wählen Sie für ACM- und IAM-Zertifikate ein Zertifikat aus.
8. Wählen Sie Als Standard speichern aus.
9. Nachdem Sie alle Listener aktualisiert haben, wählen Sie Speichern aus.

[ELB.4] Application Load Balancer sollte so konfiguriert sein, dass ungültige HTTP-Header gelöscht werden

Verwandte Anforderungen: NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8 (2), PCI DSS v4.0.1/6.2.4

Kategorie: Schützen > Netzwerksicherheit

Schweregrad: Mittel

Art der Ressource: AWS::ElasticLoadBalancingV2::LoadBalancer

AWS Config -Regel: [alb-http-drop-invalid-header-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement bewertet, ob ein Application Load Balancer so konfiguriert ist, dass er ungültige HTTP-Header löscht. Das Steuerelement schlägt fehl, wenn der Wert von auf gesetzt `routing.http.drop_invalid_header_fields.enabled` ist. `false`

Standardmäßig sind Application Load Balancer nicht so konfiguriert, dass sie ungültige HTTP-Header-Werte löschen. Durch das Entfernen dieser Header-Werte werden HTTP-Desync-Angriffe verhindert.

 Note

Wir empfehlen, diese Steuerung zu deaktivieren, wenn ELB.12 in Ihrem Konto aktiviert ist. Weitere Informationen finden Sie unter [\[ELB.12\] Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden](#).

Abhilfe

Um dieses Problem zu beheben, konfigurieren Sie Ihren Load Balancer so, dass ungültige Header-Felder gelöscht werden.

Um den Load Balancer so zu konfigurieren, dass ungültige Header-Felder gelöscht werden

1. Öffnen Sie die EC2 Amazon-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Klicken Sie im Navigationsbereich auf Load balancers (Load Balancer).
3. Wählen Sie einen Application Load Balancer aus.
4. Wählen Sie unter Aktionen die Option Attribute bearbeiten aus.
5. Wählen Sie unter Ungültige Header-Felder löschen die Option Aktivieren aus.

6. Wählen Sie Speichern.

[ELB.5] Die Protokollierung von Anwendungen und Classic Load Balancern sollte aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (26), (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-7 NIST.800-53.r5 SC-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

AWS::ElasticLoadBalancing::LoadBalancerRessourcentyp:,
AWS::ElasticLoadBalancingV2::LoadBalancer

AWS Config -Regel: [elb-logging-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der Application Load Balancer und der Classic Load Balancer die Protokollierung aktiviert haben. Ist dies der Fall, schlägt die Steuerung fehl.
`access_logs.s3.enabled false`

Elastic Load Balancing bietet Zugriffsprotokolle, die detaillierte Informationen zu Anforderungen erfassen, die an Ihren Load Balancer gesendet werden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten. Sie können diese Zugriffsprotokolle für die Analyse von Datenverkehrsmustern und zur Problembehebung verwenden.

Weitere Informationen finden Sie unter [Zugriffsprotokolle für Ihren Classic Load Balancer](#) im Benutzerhandbuch für Classic Load Balancer.

Abhilfe

Informationen zum Aktivieren von Zugriffsprotokollen finden Sie unter [Schritt 3: Zugriffsprotokolle konfigurieren](#) im Benutzerhandbuch für Application Load Balancers.

[ELB.6] Für Anwendungen, Gateways und Network Load Balancers sollte der Löschschutz aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: AWS::ElasticLoadBalancingV2::LoadBalancer

AWS Config -Regel: [elb-deletion-protection-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für eine Anwendung, ein Gateway oder ein Network Load Balancer der Löschschutz aktiviert ist. Die Steuerung schlägt fehl, wenn der Löschschutz deaktiviert ist.

Aktivieren Sie den Löschschutz, um Ihre Anwendung, Ihr Gateway oder Ihren Network Load Balancer vor dem Löschen zu schützen.

Abhilfe

Um zu verhindern, dass der Load Balancer versehentlich gelöscht wird, können Sie den Löschschutz aktivieren. Standardmäßig ist der Löschschutz für Ihren Load Balancer deaktiviert.

Wenn Sie den Löschschutz für Ihren Load Balancer aktivieren, müssen Sie den Löschschutz deaktivieren, bevor Sie den Load Balancer löschen können.

Informationen zum Aktivieren des Löschschutzes für einen Application Load Balancer finden Sie unter [Löschschutz](#) im Benutzerhandbuch für Application Load Balancer. Informationen zum Aktivieren des Löschschutzes für einen Gateway Load Balancer finden Sie unter [Löschschutz](#) im Benutzerhandbuch für Gateway Load Balancer. Informationen zum Aktivieren des Löschschutzes für einen Network Load Balancer finden Sie unter [Löschschutz](#) im Benutzerhandbuch für Network Load Balancer.

[ELB.7] Bei Classic Load Balancern sollte der Verbindungsabbau aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Erholung > Resilienz

Schweregrad: Mittel

Art der Ressource: AWS::ElasticLoadBalancing::LoadBalancer

AWS Config Regel: elb-connection-draining-enabled (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob bei Classic Load Balancern der Verbindungsabbau aktiviert ist.

Durch die Aktivierung des Verbindungsabbaus auf Classic Load Balancern wird sichergestellt, dass der Load Balancer keine Anfragen mehr an Instances sendet, die sich abmelden oder deren Status beeinträchtigt ist. Es hält die bestehenden Verbindungen offen. Dies ist besonders nützlich für Instances in Auto Scaling Scaling-Gruppen, um sicherzustellen, dass Verbindungen nicht abrupt unterbrochen werden.

Abhilfe

Informationen zum Aktivieren des Verbindungsabbaus auf Classic Load Balancern finden [Sie unter Connection Draining für Ihren Classic Load Balancer konfigurieren](#) im Benutzerhandbuch für Classic Load Balancern.

[ELB.8] Classic Load Balancer mit SSL-Listnern sollten eine vordefinierte Sicherheitsrichtlinie mit starker Dauer verwenden AWS Config

Verwandte Anforderungen: NIST.800-53.r5 AC-1 7 (2), NIST.800-53.r5 IA-5 (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 (3), 3, 3 (NIST.800-53.r5 SC-13), NIST.800-53.r5 SC-2 3 (NIST.800-53.r5 SC-23), (4), NIST.800-53.r5 SC-7 (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8 (2), NIST.800-53.R5 SI-7 (6), NIST.800-171.r2 3.13.8, NIST.800-171.r2 3.13.15, PCI DSS v4.0.1/4.2.1

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: AWS::ElasticLoadBalancing::LoadBalancer

AWS Config -Regel: [elb-predefined-security-policy-ssl-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- predefinedPolicyName: ELBSecurityPolicy-TLS-1-2-2017-01 (nicht anpassbar)

Dieses Steuerelement prüft, ob Ihre Classic Load Balancer HTTPS/SSL Balancer-Listener die vordefinierte Richtlinie verwenden. ELBSecurityPolicy-TLS-1-2-2017-01 Die Steuerung schlägt fehl, wenn die Classic Load Balancer HTTPS/SSL Balancer-Listener sie nicht verwenden. ELBSecurityPolicy-TLS-1-2-2017-01

Eine Sicherheitsrichtlinie ist eine Kombination aus SSL-Protokollen, Chiffren und der Option Server Order Preference. Vordefinierte Richtlinien steuern die Chiffren, Protokolle und Präferenzreihenfolgen, die bei SSL-Verhandlungen zwischen einem Client und einem Load Balancer unterstützt werden sollen.

Die Verwendung ELBSecurityPolicy-TLS-1-2-2017-01 kann Ihnen dabei helfen, die Compliance- und Sicherheitsstandards zu erfüllen, nach denen Sie bestimmte Versionen von SSL und TLS deaktivieren müssen. Weitere Informationen finden Sie unter [Vordefinierte SSL-Sicherheitsrichtlinien für Classic Load Balancers](#) im Benutzerhandbuch für Classic Load Balancers.

Abhilfe

Informationen zur Verwendung der vordefinierten Sicherheitsrichtlinie ELBSecurityPolicy-TLS-1-2-2017-01 mit einem Classic Load Balancer finden [Sie unter Sicherheitseinstellungen konfigurieren](#) im Benutzerhandbuch für Classic Load Balancers.

[ELB.9] Bei Classic Load Balancers sollte der zonenübergreifende Load Balancing aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: AWS::ElasticLoadBalancing::LoadBalancer

AWS Config -Regel: [elb-cross-zone-load-balancing-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der zonenübergreifende Load Balancing für die Classic Load Balancer aktiviert ist (CLBs). Die Steuerung schlägt fehl, wenn der zonenübergreifende Lastenausgleich für einen CLB nicht aktiviert ist.

Ein Load Balancer-Knoten verteilt den Verkehr nur auf die registrierten Ziele in seiner Availability Zone. Wenn zonenübergreifendes Load Balancing deaktiviert ist, verteilt jeder Load Balancer-Knoten den Datenverkehr gleichmäßig nur auf die registrierten Ziele in seiner Availability Zone. Wenn die Anzahl der registrierten Ziele in den Availability Zones nicht identisch ist, wird der Verkehr nicht gleichmäßig verteilt und die Instances in einer Zone werden möglicherweise im Vergleich zu den Instances in einer anderen Zone überlastet. Wenn zonenübergreifendes Load Balancing aktiviert ist, verteilt jeder Load Balancer-Knoten für Ihren Classic Load Balancer Anfragen gleichmäßig auf die registrierten Instances in allen aktivierten Availability Zones. Einzelheiten finden Sie unter [Zonenübergreifendes Load Balancing](#) im Elastic Load Balancing User Guide.

Abhilfe

Informationen zur Aktivierung von zonenübergreifendem Load Balancing in einem Classic Load Balancer finden Sie unter [Aktivieren von zonenübergreifendem Load Balancing](#) im Benutzerhandbuch für Classic Load Balancer.

[ELB.10] Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: AWS::ElasticLoadBalancing::LoadBalancer

AWS Config -Regel: [clb-multiple-az](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
minAvailabilityZones	Mindestanzahl von Availability Zones	Enum	2, 3, 4, 5, 6	2

Dieses Steuerelement prüft, ob ein Classic Load Balancer so konfiguriert wurde, dass er sich über mindestens die angegebene Anzahl von Availability Zones (AZs) erstreckt. Die Steuerung schlägt fehl, wenn der Classic Load Balancer nicht mindestens die angegebene Anzahl von AZs umfasst. Sofern Sie keinen benutzerdefinierten Parameterwert für die Mindestanzahl von angeben AZs, verwendet Security Hub den Standardwert AZs 2.

Ein Classic Load Balancer kann so eingerichtet werden, dass eingehende Anfragen auf EC2 Amazon-Instances in einer einzigen Availability Zone oder mehreren Availability Zones verteilt werden. Ein Classic Load Balancer, der sich nicht über mehrere Availability Zones erstreckt, kann den Traffic nicht zu Zielen in einer anderen Availability Zone umleiten, wenn die einzige konfigurierte Availability Zone nicht mehr verfügbar ist.

Abhilfe

Informationen zum Hinzufügen von Availability Zones zu einem Classic Load Balancer finden Sie unter [Hinzufügen oder Entfernen von Subnetzen für Ihren Classic Load Balancer](#) im Benutzerhandbuch für Classic Load Balancer.

[ELB.12] Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2, PCI DSS v4.0.1/6.2.4

Kategorie: Schützen > Datenschutz > Datenintegrität

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config -Regel: [alb-desync-mode-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `desyncMode`: `defensive`, `strictest` (nicht anpassbar)

Dieses Steuerelement prüft, ob ein Application Load Balancer mit dem defensiven Modus oder dem strengsten Modus zur Desynchronisierung konfiguriert ist. Die Steuerung schlägt fehl, wenn ein Application Load Balancer nicht mit dem defensiven Modus oder dem strengsten Modus zur Desynchronisierung konfiguriert ist.

Probleme mit der HTTP-Desynchronisierung können zum Schmuggel von Anfragen führen und Anwendungen anfällig für Queue-Anfragen oder Cache-Poisoning machen. Diese Sicherheitsanfälligkeiten können wiederum dazu führen, dass Anmeldeinformationen überlastet werden oder nicht autorisierte Befehle ausgeführt werden. Application Load Balancer, die mit dem defensiven Modus oder der striktesten Abschwächung der Desynchronisierung konfiguriert sind, schützen Ihre Anwendung vor Sicherheitsproblemen, die durch HTTP-Desync verursacht werden können.

Abhilfe

Informationen zum Aktualisieren des Desync-Minimationsmodus eines Application Load Balancer finden Sie unter [Desync-Minimationsmodus](#) im Benutzerhandbuch für Application Load Balancers.

[ELB.13] Anwendungs-, Netzwerk- und Gateway-Load Balancer sollten sich über mehrere Availability Zones erstrecken

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config -Regel: [elbv2-multiple-az](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
minAvailabilityZones	Mindestanzahl von Availability Zones	Enum	2, 3, 4, 5, 6	2

Dieses Steuerelement prüft, ob ein Elastic Load Balancer V2 (Application, Network oder Gateway Load Balancer) Instances aus mindestens der angegebenen Anzahl von Availability Zones (AZs) registriert hat. Die Steuerung schlägt fehl, wenn auf einem Elastic Load Balancer V2 keine Instances in mindestens der angegebenen Anzahl von AZs registriert sind. Sofern Sie keinen benutzerdefinierten Parameterwert für die Mindestanzahl von angeben AZs, verwendet Security Hub den Standardwert AZs 2.

Elastic Load Balancing verteilt Ihren eingehenden Traffic automatisch auf mehrere Ziele wie EC2 Instances, Container und IP-Adressen in einer oder mehreren Availability Zones. Elastic Load Balancing skaliert Ihren Load Balancer, wenn sich der eingehende Datenverkehr im Laufe der Zeit ändert. Es wird empfohlen, mindestens zwei Availability Zones zu konfigurieren, um die Verfügbarkeit von Diensten sicherzustellen, da der Elastic Load Balancer den Traffic in eine andere Availability Zone weiterleiten kann, falls eine nicht verfügbar ist. Durch die Konfiguration mehrerer Availability Zones wird vermieden, dass es für die Anwendung nur einen einzigen Fehlerpunkt gibt.

Abhilfe

Informationen zum Hinzufügen einer Availability Zone zu einem Application Load Balancer finden Sie unter [Availability Zones for your Application Load Balancer](#) im Benutzerhandbuch für Application Load Balancer. Informationen zum Hinzufügen einer Availability Zone zu einem Network Load Balancer finden Sie unter [Network Load Balancers](#) im Benutzerhandbuch für Network Load Balancer. Informationen zum Hinzufügen einer Availability Zone zu einem Gateway Load Balancer finden Sie [unter Erstellen eines Gateway Load Balancers](#) im Benutzerhandbuch für Gateway Load Balancer.

[ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2, PCI DSS v4.0.1/6.2.4

Kategorie: Schützen > Datenschutz > Datenintegrität

Schweregrad: Mittel

Art der Ressource: AWS::ElasticLoadBalancing::LoadBalancer

AWS Config -Regel: [clb-desync-mode-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- desyncMode: defensive, strictest (nicht anpassbar)

Dieses Steuerelement prüft, ob ein Classic Load Balancer mit einem defensiven oder dem strengsten Desync-Minimierungsmodus konfiguriert ist. Die Steuerung schlägt fehl, wenn der Classic Load Balancer nicht mit dem defensiven Modus oder dem strengsten Modus zur Desynchronisierung konfiguriert ist.

Probleme mit der HTTP-Desynchronisierung können zum Schmuggel von Anfragen führen und Anwendungen anfällig für Queue-Anfragen oder Cache-Poisoning machen. Diese Sicherheitsanfälligkeiten können wiederum zum Entführen von Anmeldeinformationen oder zur Ausführung nicht autorisierter Befehle führen. Classic Load Balancer, die mit dem defensiven Modus oder der striktesten Abschwächung der Desynchronisierung konfiguriert sind, schützen Ihre Anwendung vor Sicherheitsproblemen, die durch HTTP-Desync verursacht werden können.

Abhilfe

Informationen zum Aktualisieren des Desync-Mitigationsmodus auf einem Classic Load Balancer finden Sie unter [Ändern des Desync-Mitigationsmodus im Benutzerhandbuch für Classic Load Balancer](#).

[ELB.16] Application Load Balancers sollten mit einer Web-ACL verknüpft sein AWS WAF

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (21)

Kategorie: Schützen > Schutzdienste

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config -Regel: [alb-waf-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Application Load Balancer einer AWS WAF Classic- oder AWS WAF Web-Zugriffskontrollliste (Web-ACL) zugeordnet ist. Die Steuerung schlägt fehl, wenn das `Enabled` Feld für die AWS WAF Konfiguration auf `false` gesetzt ist.

AWS WAF ist eine Firewall für Webanwendungen, die zum Schutz von Webanwendungen und APIs vor Angriffen beiträgt. Mit AWS WAF können Sie eine Web-ACL konfigurieren, bei der es sich um eine Reihe von Regeln handelt, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Wir empfehlen, Ihren Application Load Balancer mit einer AWS WAF Web-ACL zu verknüpfen, um ihn vor böswilligen Angriffen zu schützen.

Abhilfe

Informationen zum Zuordnen eines Application Load Balancer zu einer Web-ACL finden Sie unter [Web-ACL mit einer AWS Ressource verknüpfen oder deren Zuordnung aufheben](#) im Developer Guide.AWS WAF

[ELB.17] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden

Verwandte Anforderungen: NIST.800-53.r5 AC-1 7 (2), (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 NIST.800-53.r5 IA-5 (3), 3, 3, NIST.800-53.r5 SC-1 3 (3), NIST.800-53.r5 SC-2 (4),

NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-7 (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8
NIST.800-53.R5 SI-7 NIST.800-53.r5 SC-8 (6)

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: AWS::ElasticLoadBalancingV2::Listener

AWS Config -Regel: [elbv2-predefined-security-policy-ssl-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:sslPolicies: ELBSecurityPolicy-TLS13-1-2-2021-06,
ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04, ELBSecurityPolicy-
TLS13-1-3-2021-06, ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04,
ELBSecurityPolicy-TLS13-1-2-Res-2021-06, ELBSecurityPolicy-TLS13-1-2-Res-
FIPS-2023-04 (nicht anpassbar)

Dieses Steuerelement prüft, ob der HTTPS-Listener für einen Application Load Balancer oder der TLS-Listener für einen Network Load Balancer so konfiguriert ist, dass Daten während der Übertragung mithilfe einer empfohlenen Sicherheitsrichtlinie verschlüsselt werden. Die Steuerung schlägt fehl, wenn der HTTPS- oder TLS-Listener für einen Load Balancer nicht für die Verwendung einer empfohlenen Sicherheitsrichtlinie konfiguriert ist.

Elastic Load Balancing verwendet eine SSL-Verhandlungskonfiguration, die als Sicherheitsrichtlinie bezeichnet wird, um Verbindungen zwischen einem Client und einem Load Balancer auszuhandeln. Die Sicherheitsrichtlinie spezifiziert eine Kombination von Protokollen und Chiffren. Das Protokoll stellt eine sichere Verbindung zwischen einem Client und einem Server her. Ein Verschlüsselungsverfahren ist ein Algorithmus, der eine kodierte Nachricht mithilfe von Verschlüsselungsschlüsseln erstellt. Während der Verbindungsaushandlung präsentieren der Client und der Load Balancer eine Liste von Verschlüsselungsverfahren und Protokollen, die sie jeweils unterstützen, nach Priorität sortiert. Die Verwendung einer empfohlenen Sicherheitsrichtlinie für einen Load Balancer kann Ihnen dabei helfen, Compliance- und Sicherheitsstandards einzuhalten.

Abhilfe

Informationen zu empfohlenen Sicherheitsrichtlinien und zur Aktualisierung von Listenern finden Sie in den folgenden Abschnitten der Elastic Load Balancing Balancing-Benutzerhandbücher: [Sicherheitsrichtlinien für Application Load Balancer](#), [Sicherheitsrichtlinien für Network Load Balancer](#),

[Aktualisieren eines HTTPS-Listeners für Ihren Application Load Balancer](#) und [Aktualisieren eines Listeners](#) für Ihren Network Load Balancer.

[ELB.18] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancingV2::Listener`

AWS Config -Regel: [elbv2-listener-encryption-in-transit](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der Listener für einen Application Load Balancer oder Network Load Balancer so konfiguriert ist, dass er ein sicheres Protokoll für die Verschlüsselung von Daten während der Übertragung verwendet. Die Steuerung schlägt fehl, wenn ein Application Load Balancer Balancer-Listener nicht für die Verwendung des HTTPS-Protokolls konfiguriert ist oder ein Network Load Balancer Balancer-Listener nicht für die Verwendung des TLS-Protokolls konfiguriert ist.

Um Daten zu verschlüsseln, die zwischen einem Client und einem Load Balancer übertragen werden, sollten die Elastic Load Balancer Balancer-Listener so konfiguriert werden, dass sie branchenübliche Sicherheitsprotokolle verwenden: HTTPS für Application Load Balancers oder TLS für Network Load Balancers. Andernfalls sind Daten, die zwischen einem Client und einem Load Balancer übertragen werden, anfällig für Abfangen, Manipulation und unbefugten Zugriff. Die Verwendung von HTTPS oder TLS durch einen Zuhörer entspricht den bewährten Sicherheitsverfahren und trägt dazu bei, die Vertraulichkeit und Integrität der Daten während der Übertragung zu gewährleisten. Dies ist besonders wichtig für Anwendungen, die vertrauliche Informationen verarbeiten oder Sicherheitsstandards einhalten müssen, die eine Verschlüsselung von Daten bei der Übertragung erfordern.

Abhilfe

Informationen zur Konfiguration von Sicherheitsprotokollen für Listener finden Sie in den folgenden Abschnitten der Elastic Load Balancing Balancing-Benutzerhandbücher: [Einen HTTPS-Listener](#)

[für Ihren Application Load Balancer erstellen und Einen Listener für Ihren Network Load Balancer erstellen.](#)

Security Hub für Elasticsearch

Diese AWS Security Hub Kontrollen bewerten den Elasticsearch-Service und die Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[ES.1] Bei Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein

Verwandte Anforderungen: PCI DSS v3.2.1/3.4, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 (1), (10), NIST.800-53.r5 SC-2 NIST.800-53.R5 SI-7 NIST.800-53.r5 SC-7 (6)

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: AWS::Elasticsearch::Domain

AWS Config -Regel: [elasticsearch-encrypted-at-rest](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob für Elasticsearch-Domains die Konfiguration „Verschlüsselung im Ruhezustand“ aktiviert ist. Die Prüfung schlägt fehl, wenn die Verschlüsselung im Ruhezustand nicht aktiviert ist.

Für eine zusätzliche Sicherheitsebene für Ihre sensiblen Daten sollten Sie Ihre Daten so konfigurieren OpenSearch, OpenSearch dass sie im Ruhezustand verschlüsselt werden. Elasticsearch-Domains bieten die Verschlüsselung von Daten im Ruhezustand. Die Funktion dient AWS KMS zum Speichern und Verwalten Ihrer Verschlüsselungsschlüssel. Um die Verschlüsselung durchzuführen, verwendet es den Advanced Encryption Standard-Algorithmus mit 256-Bit-Schlüsseln (AES-256).

Weitere Informationen zur OpenSearch Verschlüsselung im Ruhezustand finden Sie unter [Verschlüsselung ruhender Daten für Amazon OpenSearch Service](#) im Amazon OpenSearch Service Developer Guide.

Bestimmte Instance-Typen, wie z. B. `t.small` und `t.medium`, unterstützen die Verschlüsselung von Daten im Ruhezustand nicht. Einzelheiten finden Sie unter [Unterstützte Instance-Typen](#) im Amazon OpenSearch Service Developer Guide.

Abhilfe

Informationen zur Aktivierung der Verschlüsselung im Ruhezustand für neue und bestehende Elasticsearch-Domains finden Sie unter [Enabling encryption of data at rest](#) im Amazon OpenSearch Service Developer Guide.

[ES.2] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein

Verwandte Anforderungen: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7), (21), (11), (16) NIST.800-53.r5 AC-3, (20) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), (3) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v4.0.1/1.4.4 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen in VPC

Schweregrad: Kritisch

Art der Ressource: `AWS::Elasticsearch::Domain`

AWS Config -Regel: [elasticsearch-in-vpc-only](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob sich Elasticsearch-Domains in einer VPC befinden. Es bewertet nicht die Konfiguration des VPC-Subnetz-Routings, um den öffentlichen Zugriff zu bestimmen. Sie sollten sicherstellen, dass Elasticsearch-Domains nicht an öffentliche Subnetze angehängt sind. Informationen zu [ressourcenbasierten Richtlinien](#) finden Sie im Amazon OpenSearch Service Developer Guide. Sie sollten auch sicherstellen, dass Ihre VPC gemäß den empfohlenen bewährten Methoden konfiguriert ist. [Bewährte Sicherheitsmethoden für Ihre VPC](#) finden Sie im Amazon VPC-Benutzerhandbuch.

Elasticsearch-Domains, die in einer VPC bereitgestellt werden, können über das private AWS Netzwerk mit VPC-Ressourcen kommunizieren, ohne das öffentliche Internet durchqueren zu

müssen. Diese Konfiguration erhöht die Sicherheitslage, indem der Zugriff auf die Daten während der Übertragung eingeschränkt wird. VPCs bieten eine Reihe von Netzwerkkontrollen, um den Zugriff auf Elasticsearch-Domains zu sichern, einschließlich Netzwerk-ACL und Sicherheitsgruppen. Security Hub empfiehlt, öffentliche Elasticsearch-Domains zu migrieren, VPCs um diese Kontrollen nutzen zu können.

Abhilfe

Wenn Sie eine Domäne mit einem öffentlichen Endpunkt erstellen, können Sie sie später nicht in einer VPC platzieren. Sie müssen stattdessen eine neue Domäne erstellen und die Daten übernehmen. Umgekehrt gilt dies auch. Wenn Sie eine Domäne innerhalb einer VPC erstellen, kann sie keinen öffentlichen Endpunkt haben. Stattdessen müssen Sie entweder [eine andere Domäne erstellen](#) oder dieses Steuerelement deaktivieren.

Weitere Informationen finden Sie unter [Starten Ihrer Amazon OpenSearch Service-Domains innerhalb einer VPC](#) im Amazon OpenSearch Service Developer Guide.

[ES.3] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden

Verwandte Anforderungen: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 3, 3 (NIST.800-53.r5 SC-23), NIST.800-53.r5 SC-2 (4), NIST.800-53.r5 SC-7 (1), NIST.800-53.r5 SC-8 (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 PCI DSS v4.0.1/4.2.1

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: AWS::Elasticsearch::Domain

AWS Config -Regel: [elasticsearch-node-to-node-encryption-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für eine Elasticsearch-Domain die node-to-node Verschlüsselung aktiviert ist. Die Steuerung schlägt fehl, wenn für die Elasticsearch-Domain keine node-to-node Verschlüsselung aktiviert ist. Die Kontrolle führt auch zu fehlgeschlagenen Ergebnissen, wenn eine Elasticsearch-Version keine node-to-node Verschlüsselungsprüfungen unterstützt.

HTTPS (TLS) kann verwendet werden, um zu verhindern, dass potenzielle Angreifer den Netzwerkverkehr mit oder ähnlichen Angriffen abhören oder manipulieren. person-in-the-middle
Nur verschlüsselte Verbindungen über HTTPS (TLS) sollten zugelassen werden. Durch die Aktivierung der node-to-node Verschlüsselung für Elasticsearch-Domains wird sichergestellt, dass die Kommunikation innerhalb des Clusters während der Übertragung verschlüsselt wird.

Mit dieser Konfiguration kann es zu Leistungseinbußen kommen. Sie sollten sich der Leistungseinbußen bewusst sein und diese testen, bevor Sie diese Option aktivieren.

Abhilfe

Informationen zur Aktivierung der node-to-node Verschlüsselung für neue und bestehende Domains finden Sie unter [node-to-nodeEnabling encryption](#) im Amazon OpenSearch Service Developer Guide.

[ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7 NIST.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Kategorie: Identifizieren - Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS::Elasticsearch::Domain

AWS Config -Regel: [elasticsearch-logs-to-cloudwatch](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- logtype = 'error'(nicht anpassbar)

Dieses Steuerelement prüft, ob Elasticsearch-Domains so konfiguriert sind, dass sie CloudWatch Fehlerprotokolle an Logs senden.

Sie sollten Fehlerprotokolle für Elasticsearch-Domains aktivieren und diese CloudWatch Protokolle zur Aufbewahrung und Beantwortung an Logs senden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Abhilfe

Informationen zur Aktivierung der Protokollveröffentlichung finden Sie unter [Aktivieren der Protokollveröffentlichung \(Konsole\)](#) im Amazon OpenSearch Service Developer Guide.

[ES.5] Für Elasticsearch-Domains sollte die Audit-Protokollierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 (9), NIST.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8), PCI DSS v4.0.1/10.4.2 NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS::Elasticsearch::Domain

AWS Config Regel: elasticsearch-audit-logging-enabled (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

- `cloudWatchLogsLogGroupArnList`(nicht anpassbar). Security Hub füllt diesen Parameter nicht aus. Durch Kommas getrennte Liste von CloudWatch Logs-Log-Gruppen, die für Audit-Logs konfiguriert werden sollten.

Diese Regel gilt, NON_COMPLIANT wenn die CloudWatch Logs-Log-Gruppe der Elasticsearch-Domain in dieser Parameterliste nicht angegeben ist.

Dieses Steuerelement prüft, ob für Elasticsearch-Domains die Audit-Protokollierung aktiviert ist. Diese Kontrolle schlägt fehl, wenn für eine Elasticsearch-Domain die Audit-Protokollierung nicht aktiviert ist.

Audit-Logs sind hochgradig anpassbar. Sie ermöglichen es Ihnen, Benutzeraktivitäten auf Ihren Elasticsearch-Clustern nachzuverfolgen, einschließlich erfolgreicher und fehlgeschlagener Authentifizierungen OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.

Abhilfe

Ausführliche Anweisungen zur Aktivierung von Audit-Logs finden Sie unter [Aktivieren von Audit-Logs](#) im Amazon OpenSearch Service Developer Guide.

[ES.6] Elasticsearch-Domains sollten mindestens drei Datenknoten haben

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: AWS::Elasticsearch::Domain

AWS Config Regel: `elasticsearch-data-node-fault-tolerance` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Elasticsearch-Domänen mit mindestens drei Datenknoten konfiguriert sind und `zoneAwarenessEnabled` ist `true`.

Eine Elasticsearch-Domain benötigt aus Gründen der Hochverfügbarkeit und Fehlertoleranz mindestens drei Datenknoten. Die Bereitstellung einer Elasticsearch-Domain mit mindestens drei Datenknoten gewährleistet den Clusterbetrieb, falls ein Knoten ausfällt.

Abhilfe

Um die Anzahl der Datenknoten in einer Elasticsearch-Domain zu ändern

1. Öffnen Sie die Amazon OpenSearch Service-Konsole unter <https://console.aws.amazon.com/aos/>.
2. Wählen Sie unter Domains den Namen der Domain aus, die Sie bearbeiten möchten.
3. Wählen Sie Edit domain (Domäne bearbeiten).
4. Stellen Sie unter Datenknoten die Anzahl der Knoten auf eine Zahl ein, die größer oder gleich ist 3.

Legen Sie für Bereitstellungen mit drei Availability Zones den Wert auf ein Vielfaches von drei fest, um eine gleichmäßige Verteilung auf die Availability Zones sicherzustellen.

5. Wählen Sie Absenden aus.

[ES.7] Elasticsearch-Domänen sollten mit mindestens drei dedizierten Master-Knoten konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: AWS::Elasticsearch::Domain

AWS Config Regel: `elasticsearch-primary-node-fault-tolerance` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Elasticsearch-Domänen mit mindestens drei dedizierten Primärknoten konfiguriert sind. Diese Kontrolle schlägt fehl, wenn die Domain keine dedizierten Primärknoten verwendet. Diese Kontrolle gilt als bestanden, wenn Elasticsearch-Domänen über fünf dedizierte Primärknoten verfügen. Die Verwendung von mehr als drei Primärknoten ist jedoch möglicherweise unnötig, um das Verfügbarkeitsrisiko zu minimieren, und führt zu zusätzlichen Kosten.

Für eine Elasticsearch-Domain sind mindestens drei dedizierte Primärknoten erforderlich, um eine hohe Verfügbarkeit und Fehlertoleranz zu gewährleisten. Dedizierte Primärknotenressourcen können bei der blue/green Bereitstellung von Datenknoten belastet werden, da zusätzliche Knoten verwaltet werden müssen. Die Bereitstellung einer Elasticsearch-Domain mit mindestens drei dedizierten Primärknoten gewährleistet eine ausreichende Ressourcenkapazität des Primärknotens und den Clusterbetrieb, falls ein Knoten ausfällt.

Abhilfe

Um die Anzahl der dedizierten Primärknoten in einer OpenSearch Domain zu ändern

1. Öffnen Sie die Amazon OpenSearch Service-Konsole unter <https://console.aws.amazon.com/aos/>.
2. Wählen Sie unter Domains den Namen der Domain aus, die Sie bearbeiten möchten.
3. Wählen Sie Edit domain (Domäne bearbeiten).
4. Stellen Sie unter Dedizierte Masterknoten den Instanztyp auf den gewünschten Instanztyp ein.
5. Stellen Sie die Anzahl der Master-Knoten auf drei oder mehr ein.
6. Wählen Sie Absenden aus.

[ES.8] Verbindungen zu Elasticsearch-Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 AC-1 7 (2), (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 NIST.800-53.r5 IA-5 (3), 3, 3, 3 (NIST.800-53.r5 SC-13), NIST.800-53.r5 SC-2 (4), NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-7 (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.R5 SI-7 NIST.800-53.r5 SC-8 (6), PCI DSS v4.0.1/4.2.1

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: AWS::Elasticsearch::Domain

AWS Config Regel: elasticsearch-https-required (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dadurch wird geprüft, ob ein Elasticsearch-Domain-Endpunkt so konfiguriert ist, dass er die neueste TLS-Sicherheitsrichtlinie verwendet. Die Steuerung schlägt fehl, wenn der Elasticsearch-Domänenendpunkt nicht für die Verwendung der neuesten unterstützten Richtlinie konfiguriert ist oder wenn er HTTPS nicht aktiviert ist. Die aktuell neueste unterstützte TLS-Sicherheitsrichtlinie ist Policy-Min-TLS-1-2-PFS-2023-10.

HTTPS (TLS) kann verwendet werden, um zu verhindern, dass potenzielle Angreifer person-in-the-middle oder ähnliche Angriffe verwenden, um den Netzwerkverkehr zu belauschen oder zu manipulieren. Nur verschlüsselte Verbindungen über HTTPS (TLS) sollten zugelassen werden. Die Verschlüsselung von Daten während der Übertragung kann die Leistung beeinträchtigen. Sie sollten Ihre Anwendung mit dieser Funktion testen, um das Leistungsprofil und die Auswirkungen von TLS zu verstehen. TLS 1.2 bietet mehrere Sicherheitsverbesserungen gegenüber früheren Versionen von TLS.

Abhilfe

Um die TLS-Verschlüsselung zu aktivieren, verwenden Sie den [UpdateDomainConfig](#) API-Vorgang, um das [DomainEndpointOptions](#) Objekt zu konfigurieren. Dies legt die `festTLSSecurityPolicy` fest.

[ES.9] Elasticsearch-Domains sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Elasticsearch::Domain`

AWS Config Regel: `tagged-elasticsearch-domain` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplanytyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob eine Elasticsearch-Domain Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind. `requiredTagKeys` Das Steuerelement schlägt fehl, wenn die Domain keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Domain mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `aws:iam:aws:iam` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Elasticsearch-Domain finden Sie unter [Arbeiten mit Tags](#) im Amazon OpenSearch Service Developer Guide.

Security Hub-Steuerelemente für Amazon EMR

Diese AWS Security Hub Kontrollen bewerten den Service und die Ressourcen von Amazon EMR (früher Amazon Elastic genannt MapReduce). Die Kontrollen sind möglicherweise nicht in allen

AWS-Regionen verfügbar. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben

Verwandte Anforderungen: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, PCI DSS v4.0.1/1.4.4, NIST.800-53.r5 AC-2 1,, NIST.800-53.r5 AC-3 (7),, (21), (21), (11) NIST.800-53.r5 AC-3, (16), (20) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-6, (3)) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Hoch

Art der Ressource: AWS::EMR::Cluster

AWS Config Regel: emr-master-no-public [-ip](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob Master-Knoten auf Amazon EMR-Clustern öffentliche IP-Adressen haben. Die Kontrolle schlägt fehl, wenn öffentliche IP-Adressen einer der Master-Node-Instances zugeordnet sind.

Öffentliche IP-Adressen werden im `PublicIp` Feld der `NetworkInterfaces` Konfiguration für die Instanz angegeben. Dieses Steuerelement überprüft nur Amazon EMR-Cluster, die sich im `WAITING` Status `RUNNING` oder befinden.

Abhilfe

Während des Starts können Sie steuern, ob Ihrer Instance in einem standardmäßigen oder einem anderen Subnetz eine öffentliche Adresse zugewiesen wird. IPv4 In Standard-Subnetzen ist dieses Attribut standardmäßig auf `gesetzt`. `true` Bei nicht standardmäßigen Subnetzen ist das IPv4 öffentliche Adressierungsattribut auf `gesetztfalse`, sofern es nicht vom Amazon EC2 Launch Instance Wizard erstellt wurde. In diesem Fall ist das Attribut auf `gesetzt`. `true`

Nach dem Start können Sie eine öffentliche IPv4 Adresse nicht manuell von Ihrer Instance trennen.

Um ein fehlgeschlagenes Ergebnis zu beheben, müssen Sie einen neuen Cluster in einer VPC mit einem privaten Subnetz starten, für das das IPv4 öffentliche Adressierungsattribut auf gesetzt ist. false Anweisungen finden Sie unter [Cluster in einer VPC starten](#) im Amazon EMR Management Guide.

[EMR.2] Die Amazon EMR-Einstellung zum Blockieren des öffentlichen Zugriffs sollte aktiviert sein

Verwandte Anforderungen: PCI DSS v4.0.1/1.4.4, NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3, (21) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6, (16) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Kategorie: Schützen > Sichere Zugriffsverwaltung > Ressource nicht öffentlich zugänglich

Schweregrad: Kritisch

Art der Ressource: AWS : : : Account

AWS Config -Regel: [emr-block-public-access](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob Ihr Konto mit Amazon EMR konfiguriert ist, um den öffentlichen Zugriff zu blockieren. Die Kontrolle schlägt fehl, wenn die Einstellung „Öffentlichen Zugriff blockieren“ nicht aktiviert ist oder wenn ein anderer Port als Port 22 zulässig ist.

Amazon EMR Block Public Access verhindert, dass Sie einen Cluster in einem öffentlichen Subnetz starten, wenn der Cluster über eine Sicherheitskonfiguration verfügt, die eingehenden Datenverkehr von öffentlichen IP-Adressen an einem Port zulässt. Wenn ein Benutzer von Ihrem AWS-Konto einen Cluster startet, überprüft Amazon EMR die Portregeln in der Sicherheitsgruppe für den Cluster und vergleicht sie mit Ihren Regeln für eingehenden Datenverkehr. Wenn die Sicherheitsgruppe über eine Regel für eingehenden Datenverkehr verfügt, die Ports zu den öffentlichen IP-Adressen IPv4 0.0.0.0/0 oder IPv6 : : /0 öffnet, und diese Ports nicht als Ausnahmen für Ihr Konto angegeben sind, lässt Amazon EMR den Benutzer den Cluster nicht erstellen.

 Note

Den öffentlichen Zugriff blockieren ist standardmäßig aktiviert. Um den Kontoschutz zu erhöhen, empfehlen wir, ihn aktiviert zu lassen.

Abhilfe

Informationen zur Konfiguration von Block Public Access für Amazon EMR finden Sie unter [Using Amazon EMR block public access](#) im Amazon EMR Management Guide.

[EMR.3] Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CP-9 (8), NIST.800-53.R5 SI-12

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: AWS::EMR::SecurityConfiguration

AWS Config -Regel: [emr-security-configuration-encryption-rest](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für eine Amazon EMR-Sicherheitskonfiguration die Verschlüsselung im Ruhezustand aktiviert ist. Die Kontrolle schlägt fehl, wenn die Sicherheitskonfiguration die Verschlüsselung im Ruhezustand nicht aktiviert.

Daten im Ruhezustand beziehen sich auf Daten, die für einen beliebigen Zeitraum in einem persistenten, nichtflüchtigen Speicher gespeichert werden. Durch die Verschlüsselung ruhender Daten können Sie deren Vertraulichkeit schützen, wodurch das Risiko verringert wird, dass ein nicht autorisierter Benutzer darauf zugreifen kann.

Abhilfe

Informationen zur Aktivierung der Verschlüsselung im Ruhezustand in einer Amazon EMR-Sicherheitskonfiguration finden [Sie unter Datenverschlüsselung konfigurieren](#) im Amazon EMR Management Guide.

[EMR.4] Amazon EMR-Sicherheitskonfigurationen sollten bei der Übertragung verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-7 (4) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-1 3, 3, NIST.800-53.r5 SC-2 3 (NIST.800-53.r5 SC-23)

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: AWS::EMR::SecurityConfiguration

AWS Config -Regel: [emr-security-configuration-encryption-transit](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob in einer Amazon EMR-Sicherheitskonfiguration die Verschlüsselung bei der Übertragung aktiviert ist. Die Kontrolle schlägt fehl, wenn die Sicherheitskonfiguration die Verschlüsselung bei der Übertragung nicht aktiviert.

Daten bei der Übertragung beziehen sich auf Daten, die von einem Standort an einen anderen übertragen werden, z. B. zwischen Knoten in Ihrem Cluster oder zwischen Ihrem Cluster und Ihrer Anwendung. Daten können über das Internet oder innerhalb eines privaten Netzwerks übertragen werden. Durch die Verschlüsselung von Daten während der Übertragung wird das Risiko verringert, dass ein nicht autorisierter Benutzer den Netzwerkverkehr abhören kann.

Abhilfe

Informationen zur Aktivierung der Verschlüsselung bei der Übertragung in einer Amazon EMR-Sicherheitskonfiguration finden [Sie unter Datenverschlüsselung konfigurieren](#) im Amazon EMR Management Guide.

Security Hub-Steuerungen für EventBridge

Diese AWS Security Hub Kontrollen bewerten den EventBridge Service und die Ressourcen von Amazon.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[EventBridge.2] EventBridge Eventbusse sollten gekennzeichnet sein

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Events::EventBus`

AWS Config Regel: `tagged-events-eventbus` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein EventBridge Amazon-Event-Bus Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind `requiredTagKeys`. Die Steuerung schlägt fehl, wenn der Event-Bus keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das

Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Event-Bus mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EventBridge Event-Bus finden Sie unter [EventBridge Amazon-Tags](#) im EventBridge Amazon-Benutzerhandbuch.

[EventBridge.3] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden

Verwandte Anforderungen: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7),, NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6 (3) NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6, PCI DSS v4.0.1/10.3.1

Kategorie: Schützen > Sichere Zugriffsverwaltung > Ressource nicht öffentlich zugänglich

Schweregrad: Niedrig

Art der Ressource: AWS::Events::EventBus

AWS Config -Regel: [custom-eventbus-policy-attached](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein EventBridge benutzerdefinierter Amazon Event Bus mit einer ressourcenbasierten Richtlinie verknüpft ist. Diese Steuerung schlägt fehl, wenn dem benutzerdefinierten Event-Bus keine ressourcenbasierte Richtlinie zugewiesen wurde.

Standardmäßig ist an einen EventBridge benutzerdefinierten Ereignisbus keine ressourcenbasierte Richtlinie angehängt. Dadurch können die Principals im Konto auf den Event-Bus zugreifen. Indem Sie eine ressourcenbasierte Richtlinie an den Event-Bus anhängen, können Sie den Zugriff auf den Event-Bus auf bestimmte Konten beschränken und Entitäten in einem anderen Konto bewusst Zugriff gewähren.

Abhilfe

Informationen zum Anhängen einer ressourcenbasierten Richtlinie an einen EventBridge benutzerdefinierten Event-Bus finden Sie unter [Using Resource Based Policies for Amazon EventBridge im Amazon-Benutzerhandbuch](#). EventBridge

[EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: AWS::Events::Endpoint

AWS Config -Regel: [global-endpoint-event-replication-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Ereignisreplikation für einen EventBridge globalen Amazon-Endpunkt aktiviert ist. Die Steuerung schlägt fehl, wenn die Ereignisreplikation für einen globalen Endpunkt nicht aktiviert ist.

Globale Endpunkte tragen dazu bei, dass Ihre Anwendung regional fehlertolerant ist. Zunächst weisen Sie dem Endpunkt eine Amazon-Route-53-Zustandsprüfung zu. Wenn ein Failover initiiert wird, meldet die Integritätsprüfung einen „fehlerhaften“ Zustand. Innerhalb weniger Minuten nach der Einleitung des Failovers werden alle benutzerdefinierten Ereignisse an einen Event Bus in der sekundären Region weitergeleitet und von diesem Event Bus verarbeitet. Wenn Sie globale Endpunkte verwenden, können Sie die Ereignisreplikation aktivieren. Bei der Ereignisreplikation werden alle benutzerdefinierten Ereignisse mithilfe verwalteter Regeln an die Event Buses in der primären und sekundären Region gesendet. Wir empfehlen, die Ereignisreplikation bei der Einrichtung globaler Endgeräte zu aktivieren. Mithilfe der Ereignisreplikation können Sie überprüfen, ob Ihre globalen Endpunkte korrekt konfiguriert sind. Für die automatische Wiederherstellung nach einem Failover-Ereignis ist die Ereignisreplikation erforderlich. Wenn Sie die Ereignisreplikation nicht aktiviert haben, müssen Sie die Route 53-Zustandsprüfung manuell auf „Fehlerfrei“ zurücksetzen, bevor Ereignisse zurück in die primäre Region umgeleitet werden.

 Note

Wenn Sie benutzerdefinierte Ereignisbusse verwenden, benötigen Sie in jeder Region einen benutzerdefinierten geraden Bus mit demselben Namen und demselben Konto, damit der Failover ordnungsgemäß funktioniert. Wenn Sie die Ereignisreplikation aktivieren, können sich Ihre monatlichen Kosten erhöhen. Informationen zu den Preisen finden Sie unter [EventBridge Amazon-Preise](#).

Abhilfe

Informationen zum Aktivieren der Ereignisreplikation für EventBridge globale Endgeräte finden [Sie unter Erstellen eines globalen Endpunkts](#) im EventBridge Amazon-Benutzerhandbuch. Wählen Sie für die Ereignisreplikation die Option Ereignisreplikation aktiviert aus.

Security Hub-Steuerelemente für Amazon Fraud Detector

Diese Security Hub Hub-Kontrollen bewerten den Service und die Ressourcen von Amazon Fraud Detector.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[FraudDetector.1] Entitätstypen von Amazon Fraud Detector sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::FraudDetector::EntityType`

AWS Config -Regel: `frauddetector-entity-type-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Entitätstyp von Amazon Fraud Detector Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind `requiredKeyTags`. Die Kontrolle schlägt fehl, wenn der Entitätstyp keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat `requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Entitätstyp mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `aws:` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck,

Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

So fügen Sie Tags zu einem Amazon Fraud Detector Detector-Entitätstyp hinzu (Konsole)

1. Öffnen Sie die Amazon Fraud Detector Detector-Konsole unter <https://console.aws.amazon.com/frauddetector>.
2. Wählen Sie im Navigationsbereich Entitäten aus.
3. Wählen Sie einen Entitätstyp aus der Liste aus.
4. Wählen Sie im Abschnitt Entitätstyp-Tags die Option Tags verwalten aus.
5. Wählen Sie Neues Tag hinzufügen aus. Geben Sie den Schlüssel und den Wert für den Tags (Markierungen) ein. Wiederholen Sie den Vorgang für weitere Schlüssel-Wert-Paare.
6. Wenn Sie mit dem Hinzufügen der Tags fertig sind, wählen Sie Speichern.

[FraudDetector.2] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::FraudDetector::Label`

AWS Config -Regel: `frauddetector-label-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Diese Kontrolle prüft, ob ein Amazon Fraud Detector-Label Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind `requiredKeyTags`. Die Kontrolle schlägt fehl, wenn das Etikett keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel enthält `requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Label mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `aws:` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen

anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

So fügen Sie Tags zu einem Amazon Fraud Detector-Label hinzu (Konsole)

1. Öffnen Sie die Amazon Fraud Detector Konsole unter <https://console.aws.amazon.com/frauddetector>.
2. Wählen Sie im Navigationsbereich Labels aus.
3. Wählen Sie ein Etikett aus der Liste aus.
4. Wählen Sie im Bereich Label-Tags die Option Tags verwalten aus.
5. Wählen Sie Neues Tag hinzufügen aus. Geben Sie den Schlüssel und den Wert für den Tags (Markierungen) ein. Wiederholen Sie den Vorgang für weitere Schlüssel-Wert-Paare.
6. Wenn Sie mit dem Hinzufügen der Tags fertig sind, wählen Sie Speichern.

[FraudDetector.3] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::FraudDetector::Outcome

AWS Config -Regel: `frauddetector-outcome-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Diese Kontrolle prüft, ob ein Ergebnis von Amazon Fraud Detector Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind `requiredKeyTags`. Die Kontrolle schlägt fehl, wenn das Ergebnis keine Tag-Schlüssel enthält oder wenn es nicht alle im Parameter angegebenen Schlüssel enthält `requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Ergebnis mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

So fügen Sie Tags zu einem Ergebnis von Amazon Fraud Detector hinzu (Konsole)

1. Öffnen Sie die Amazon Fraud Detector Konsole unter <https://console.aws.amazon.com/frauddetector>.
2. Wählen Sie im Navigationsbereich Outcomes aus.
3. Wählen Sie ein Ergebnis aus der Liste aus.
4. Wählen Sie im Abschnitt Ergebnis-Tags die Option Tags verwalten aus.
5. Wählen Sie Neues Tag hinzufügen aus. Geben Sie den Schlüssel und den Wert für den Tags (Markierungen) ein. Wiederholen Sie den Vorgang für weitere Schlüssel-Wert-Paare.
6. Wenn Sie mit dem Hinzufügen der Tags fertig sind, wählen Sie Speichern.

[FraudDetector.4] Amazon Fraud Detector Detector-Variablen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::FraudDetector::Variable`

AWS Config -Regel: `frauddetector-variable-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon Fraud Detector Detector-Variable Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind `requiredKeyTags`. Die Steuerung schlägt fehl, wenn die Variable keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat `requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Variable mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

So fügen Sie Tags zu einer Amazon Fraud Detector Detector-Variablen hinzu (Konsole)

1. Öffnen Sie die Amazon Fraud Detector Detector-Konsole unter <https://console.aws.amazon.com/frauddetector>.
2. Wählen Sie im Navigationsbereich Variablen aus.
3. Wählen Sie eine Variable aus der Liste aus.
4. Wählen Sie im Bereich Variablen-Tags die Option Tags verwalten aus.
5. Wählen Sie Neues Tag hinzufügen aus. Geben Sie den Schlüssel und den Wert für den Tags (Markierungen) ein. Wiederholen Sie den Vorgang für weitere Schlüssel-Wert-Paare.
6. Wenn Sie mit dem Hinzufügen der Tags fertig sind, wählen Sie Speichern.

Security Hub-Steuerelemente für Amazon FSx

Diese AWS Security Hub Kontrollen bewerten den FSx Service und die Ressourcen von Amazon. Die Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[FSx.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2)

Kategorie: Identifizieren > Inventar > Etikettieren

Schweregrad: Niedrig

Art der Ressource: AWS::FSx::FileSystem

AWS Config -Regel: [fsx-openzfs-copy-tags-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon FSx for OpenZFS-Dateisystem so konfiguriert ist, dass es Tags auf Backups und Volumes kopiert. Die Kontrolle schlägt fehl, wenn das OpenZFS-Dateisystem nicht so konfiguriert ist, dass es Tags auf Backups und Volumes kopiert.

Die Identifizierung und Inventarisierung Ihrer IT-Ressourcen ist ein wichtiger Aspekt der Unternehmensführung und Sicherheit. Mithilfe von Tags können Sie Ihre AWS Ressourcen auf unterschiedliche Weise kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung. Dies ist nützlich, wenn Sie über viele Ressourcen desselben Typs verfügen, da Sie eine bestimmte Ressource anhand der Tags, die Sie ihr zugewiesen haben, schnell identifizieren können.

Abhilfe

Informationen zur Konfiguration eines Dateisystems FSx für OpenZFS zum Kopieren von Tags auf Backups und Volumes finden Sie unter [Aktualisieren eines Dateisystems](#) im Amazon FSx for OpenZFS-Benutzerhandbuch.

[FSx.2] FSx für Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden

Verwandte Anforderungen: NIST.800-53.R5 CP-9, NIST.800-53.R5 CM-8

Kategorie: Identifizieren > Inventar > Etikettieren

Schweregrad: Niedrig

Art der Ressource: AWS::FSx::FileSystem

AWS Config -Regel: [fsx-lustre-copy-tags-to-backups](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon FSx for Lustre-Dateisystem so konfiguriert ist, dass es Tags auf Backups und Volumes kopiert. Die Kontrolle schlägt fehl, wenn das Lustre-Dateisystem nicht so konfiguriert ist, dass es Tags auf Backups und Volumes kopiert.

Die Identifizierung und Inventarisierung Ihrer IT-Ressourcen ist ein wichtiger Aspekt der Unternehmensführung und Sicherheit. Mithilfe von Tags können Sie Ihre AWS Ressourcen auf unterschiedliche Weise kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung. Dies ist nützlich, wenn Sie über viele Ressourcen desselben Typs verfügen, da Sie eine bestimmte Ressource anhand der Tags, die Sie ihr zugewiesen haben, schnell identifizieren können.

Abhilfe

Informationen zur Konfiguration eines FSx for Lustre-Dateisystems zum Kopieren von Tags in Backups finden Sie unter [Kopieren von Backups innerhalb desselben AWS-Konto](#) im Amazon FSx for Lustre-Benutzerhandbuch.

[FSx.3] FSx für OpenZFS-Dateisysteme sollte für die Multi-AZ-Bereitstellung konfiguriert werden

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: AWS::FSx::FileSystem

AWS Config -Regel: [fsx-openzfs-deployment-type-check](#)

Art des Zeitplans: Periodisch

Parameter: deploymentTypes: MULTI_AZ_1 (nicht anpassbar)

Dieses Steuerelement prüft, ob ein Amazon FSx for OpenZFS-Dateisystem für die Verwendung des Bereitstellungstyps „Mehrere Availability Zones“ (Multi-AZ) konfiguriert ist. Die Steuerung schlägt fehl, wenn das Dateisystem nicht für die Verwendung des Multi-AZ-Bereitstellungstyps konfiguriert ist.

Amazon FSx für OpenZFS unterstützt mehrere Bereitstellungstypen für Dateisysteme: Multi-AZ (HA), Single-AZ (HA) und Single-AZ (Non-HA). Die Bereitstellungstypen bieten unterschiedliche Verfügbarkeits- und Haltbarkeitsstufen. Multi-AZ-Dateisysteme (HA) bestehen aus zwei Dateiservern mit hoher Verfügbarkeit (HA), die über zwei Availability Zones (AZs) verteilt sind. Wir empfehlen die Verwendung des Bereitstellungstyps Multi-AZ (HA) für die meisten Produktionsworkloads aufgrund des damit verbundenen Hochverfügbarkeits- und Stabilitätsmodells.

Abhilfe

Sie können ein Amazon FSx for OpenZFS-Dateisystem so konfigurieren, dass es den Multi-AZ-Bereitstellungstyp verwendet, wenn Sie das Dateisystem erstellen. Sie können den Bereitstellungstyp für ein FSx für OpenZFS vorhandenes Dateisystem nicht ändern.

Informationen zu Bereitstellungstypen und Optionen FSx für OpenZFS-Dateisysteme finden Sie unter [Verfügbarkeit und Haltbarkeit von Amazon FSx für OpenZFS](#) und [Verwaltung von Dateisystemressourcen](#) im Amazon FSx for OpenZFS-Benutzerhandbuch.

[FSx.4] FSx für NetApp ONTAP-Dateisysteme sollte für die Multi-AZ-Bereitstellung konfiguriert sein

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: AWS::FSx::FileSystem

AWS Config -Regel: [fsx-ontap-deployment-type-check](#)

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
deploymentTypes	Eine Liste der Bereitstellungstypen, die in die Bewertung einbezogen werden sollen. Das Steuerelement generiert einen FAILED Befund, wenn ein Dateisystem nicht für die Verwendung eines in der Liste angegebenen Bereitstellungstyps konfiguriert ist.	Enum	MULTI_AZ_1 , MULTI_AZ_2	MULTI_AZ_1 , MULTI_AZ_2

Diese Kontrolle prüft, ob ein Amazon FSx for NetApp ONTAP-Dateisystem für die Verwendung eines Bereitstellungstyps mit mehreren Availability Zones (Multi-AZ) konfiguriert ist. Die Steuerung schlägt fehl, wenn das Dateisystem nicht für die Verwendung eines Multi-AZ-Bereitstellungstyps konfiguriert ist. Sie können optional eine Liste von Bereitstellungstypen angeben, die in die Bewertung einbezogen werden sollen.

Amazon FSx for NetApp ONTAP unterstützt mehrere Bereitstellungstypen für Dateisysteme: Single-AZ 1, Single-AZ 2, Multi-AZ 1 und Multi-AZ 2. Die Bereitstellungstypen bieten unterschiedliche Verfügbarkeits- und Haltbarkeitsstufen. Wir empfehlen die Verwendung eines Multi-AZ-Bereitstellungstyps für die meisten Produktionsworkloads, da Multi-AZ-Bereitstellungstypen ein Modell mit hoher Verfügbarkeit und Haltbarkeit bieten. Multi-AZ-Dateisysteme unterstützen alle Verfügbarkeits- und Haltbarkeitsfunktionen von Single-AZ-Dateisystemen. Darüber hinaus sind sie so konzipiert, dass Daten auch dann kontinuierlich verfügbar sind, wenn eine Availability Zone (AZ) nicht verfügbar ist.

Abhilfe

Sie können den Bereitstellungstyp für ein vorhandenes Amazon FSx for NetApp ONTAP-Dateisystem nicht ändern. Sie können die Daten jedoch sichern und sie dann auf einem neuen Dateisystem wiederherstellen, das einen Multi-AZ-Bereitstellungstyp verwendet.

Informationen zu Bereitstellungstypen und Optionen FSx für ONTAP-Dateisysteme finden Sie unter [Verfügbarkeit, Haltbarkeit und Bereitstellungsoptionen und Verwaltung von Dateisystemen](#) im FSx for ONTAP-Benutzerhandbuch.

[FSx.5] FSx für Windows-Dateiserver sollten für die Multi-AZ-Bereitstellung konfiguriert sein

Kategorie: Wiederherstellen > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: AWS::FSx::FileSystem

AWS Config -Regel: [fsx-windows-deployment-type-check](#)

Art des Zeitplans: Periodisch

Parameter: deploymentTypes: MULTI_AZ_1 (nicht anpassbar)

Dieses Steuerelement prüft, ob ein Dateisystem von Amazon FSx für Windows File Server so konfiguriert ist, dass es den Bereitstellungstyp Multi-AZ (Multi-AZ) verwendet. Die Steuerung schlägt fehl, wenn das Dateisystem nicht für die Verwendung des Multi-AZ-Bereitstellungstyps konfiguriert ist.

Amazon FSx for Windows File Server unterstützt zwei Bereitstellungstypen für Dateisysteme: Single-AZ und Multi-AZ. Die Bereitstellungstypen bieten unterschiedliche Verfügbarkeits- und Haltbarkeitsstufen. Single-AZ-Dateisysteme bestehen aus einer einzelnen Windows-Dateiserverinstanz und einer Reihe von Speichervolumen innerhalb einer einzigen Availability Zone (AZ). Multi-AZ-Dateisysteme bestehen aus einem Hochverfügbarkeitscluster von Windows-Dateiservern, die auf zwei Availability Zones verteilt sind. Wir empfehlen die Verwendung des Multi-AZ-Bereitstellungstyps für die meisten Produktionsworkloads aufgrund des damit verbundenen Hochverfügbarkeits- und Haltbarkeitsmodells.

Abhilfe

Sie können ein Dateisystem von Amazon FSx für Windows so konfigurieren, dass es den Multi-AZ-Bereitstellungstyp verwendet, wenn Sie das Dateisystem erstellen. Sie können den Bereitstellungstyp für ein vorhandenes Dateisystem FSx für Windows File Server nicht ändern.

Informationen zu Bereitstellungstypen und Optionen FSx für Windows File Server-Dateisysteme finden Sie unter [Verfügbarkeit und Haltbarkeit: Single-AZ- und Multi-AZ-Dateisysteme](#) und [Erste Schritte mit Amazon FSx for Windows File Server](#) im Amazon FSx for Windows File Server-Benutzerhandbuch.

Security Hub-Steuerungen für Global Accelerator

Diese AWS Security Hub Kontrollen bewerten den AWS Global Accelerator Service und die Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::GlobalAccelerator::Accelerator

AWS Config Regel: tagged-globalaccelerator-accelerator (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob ein AWS Global Accelerator Accelerator über Tags mit den spezifischen Tasten verfügt, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn der Beschleuniger keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Beschleuniger mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen

möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Global Accelerator Global Accelerator finden Sie unter [Tagging in AWS Global Accelerator im AWS Global Accelerator Developer Guide](#).

Security Hub-Steuerungen für AWS Glue

Diese AWS Security Hub Kontrollen bewerten den AWS Glue Service und die Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[Glue.1] AWS Glue Jobs sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::Glue::Job

AWS Config Regel: tagged-glue-job (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS Glue Job über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn der Job keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Job mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `aws:*` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Stichwörtern zu einem AWS Glue Job finden Sie unter [AWS Stichwörter AWS Glue im AWS Glue](#) Benutzerhandbuch.

[Glue.3] Transformationen für AWS Glue maschinelles Lernen sollten im Ruhezustand verschlüsselt werden

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: AWS::Glue::MLTransform

AWS Config -Regel: [glue-ml-transform-encrypted-at-rest](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Nein

Dieses Steuerelement prüft, ob eine Transformation für AWS Glue maschinelles Lernen im Ruhezustand verschlüsselt ist. Die Steuerung schlägt fehl, wenn die Transformation für maschinelles Lernen im Ruhezustand nicht verschlüsselt ist.

Daten im Ruhezustand beziehen sich auf Daten, die für einen beliebigen Zeitraum in einem persistenten, nichtflüchtigen Speicher gespeichert werden. Durch die Verschlüsselung ruhender Daten können Sie deren Vertraulichkeit schützen, wodurch das Risiko verringert wird, dass ein nicht autorisierter Benutzer darauf zugreifen kann.

Abhilfe

Informationen zur Konfiguration der Verschlüsselung für AWS Glue Machine-Learning-Transformationen finden Sie unter [Arbeiten mit Transformationen für maschinelles Lernen](#) im AWS Glue Benutzerhandbuch.

[Glue.4] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), NIST.800-53.R5 SI-2 (5)

Kategorie: Identifizieren > Schwachstellen-, Patch- und Versionsverwaltung

Schweregrad: Mittel

Art der Ressource: AWS::Glue::Job

AWS Config -Regel: [glue-spark-job-supported-version](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:minimumSupportedGlueVersion: 3.0 (nicht anpassbar)

Dieses Steuerelement prüft, ob ein AWS Glue for Spark-Job so konfiguriert ist, dass er auf einer unterstützten Version von ausgeführt wird AWS Glue. Die Steuerung schlägt fehl, wenn der Spark-Job so konfiguriert ist AWS Glue , dass er auf einer älteren Version als der unterstützten Mindestversion ausgeführt wird.

Note

Dieses Steuerelement generiert auch einen FAILED Befund AWS Glue für einen Spark-Job, wenn die Eigenschaft AWS Glue version (GlueVersion) nicht existiert oder im Configuration Item (CI) für den Job Null ist. In solchen Fällen enthält das Ergebnis die folgende Anmerkung:GlueVersion is null or missing in glueetl job configuration. Um diese Art von FAILED Befund zu beheben, fügen Sie die GlueVersion Eigenschaft der Konfiguration des Jobs hinzu. Eine Liste der unterstützten Versionen und Laufzeitumgebungen finden Sie im AWS Glue Benutzerhandbuch unter [AWS Glue Versionen](#).

Das Ausführen von AWS Glue Spark-Jobs auf aktuellen Versionen von AWS Glue kann die Leistung, Sicherheit und den Zugriff auf die neuesten Funktionen von optimieren AWS Glue. Es kann auch zum Schutz vor Sicherheitslücken beitragen. Beispielsweise kann eine neue Version veröffentlicht werden, um Sicherheitsupdates bereitzustellen, Probleme zu beheben oder neue Funktionen einzuführen.

Abhilfe

Informationen zur Migration eines Spark-Jobs zu einer unterstützten Version von AWS Glue finden Sie unter [Migration AWS Glue für Spark-Jobs](#) im AWS Glue Benutzerhandbuch.

Security Hub Hub-Kontrollen für Amazon GuardDuty

Diese AWS Security Hub Kontrollen bewerten den GuardDuty Service und die Ressourcen von Amazon. Die Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[GuardDuty.1] GuardDuty sollte aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (12), (4), 1 (1) NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(5), NIST.800-53.r5 CA-7, NIST.800-53.r5 SA-1 1 NIST.800-53.r5 CM-8(3), NIST.800-53.r5 RA-3 (6), 5 (2), NIST.800-53.r5 SA-1 5 (8), (19), (21), (25),, (NIST.800-53.r5 SA-11), (3), NIST.800-53.r5 SA-1 Nist.800-53.R5 SI-20, NIST.800-53.r5 SA-8 NIST.800-53.R5 SI-3 NIST.800-53.r5 SA-8 (8) NIST.800-53.r5 SC-5, NIST.800-53.r5 SC-5 Nist.800-53.R5 SI-4, NIST.800-53.R5 R5 SI-4 NIST.800-53.r5 SC-5 (1), NIST.800-53.R5 SI-4 (13), NIST.800-53.R5 SI-4 (2), NIST.800-53.R5 SI-4 (22), NIST.800-53.R5 SI-4 (25), Nist.800-53.R5 SI-4 (4), Nist.800-53.r5 SI-4 (5), Nist.800-171.r2 3.4.2, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7, PCI DSS v3.2.1/11.4 NIST.800-53.r5 SA-8 , PCI DSS v4.0.1/11.5.1

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Hoch

Art der Ressource: AWS : : : Account

AWS Config -Regel: [guardduty-enabled-centralized](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob Amazon in Ihrem GuardDuty Konto und Ihrer Region aktiviert GuardDuty ist.

Es wird dringend empfohlen, die Aktivierung GuardDuty in allen unterstützten AWS Regionen durchzuführen. Dadurch können GuardDuty sogar in Regionen, die Sie nicht aktiv verwenden, Erkenntnisse über nicht autorisierte oder ungewöhnliche Aktivitäten generieren. Dies ermöglicht auch GuardDuty die Überwachung globaler CloudTrail Ereignisse AWS-Services wie IAM.

Abhilfe

Informationen zur Aktivierung GuardDuty finden Sie unter [Erste Schritte mit GuardDuty](#) im GuardDuty Amazon-Benutzerhandbuch.

[GuardDuty.2] GuardDuty Filter sollten mit Tags versehen sein

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::GuardDuty::Filter`

AWS Config Regel: `tagged-guardduty-filter` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Allowed Werte	Security Hub: Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob ein GuardDuty Amazon-Filter Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind `requiredTagKeys`. Das Steuerelement schlägt fehl, wenn der Filter keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Filter mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `aws:` beginnen, werden ignoriert.

Ein Tag (Markierung) ist eine Markierung, die Sie einer AWS -Ressource zuordnen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach

Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Tags können Ihnen helfen, -Ressourcen zu identifizieren, Tags können Ihnen helfen, -Ressourcen zu identifizieren, um -Ressourcen zu identifizieren, um -Ressourcen zu identifizieren Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, die Berechtigungen basierend auf Tags definiert. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an AWS -Ressourcen anfügen. Sie können eine einzelne ABAC-Richtlinie oder einen separaten Richtlinienatz für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen zugelassen werden, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Was ist ABAC für AWS?](#) im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbare Informationen (PII) oder andere vertrauliche Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, einschließlich AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem GuardDuty Filter finden Sie [TagResource](#) in der Amazon GuardDuty API-Referenz.

[GuardDuty.3] GuardDuty IPSets sollte markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::GuardDuty::IPSet

AWS Config Regel: tagged-guarddduty-ipset (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Allowed Werte	Security Hub: Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob ein Amazon Tag mit den spezifischen Schlüsseln GuardDuty IPSet hat, die im Parameter definiert sind `requiredTagKeys`. Das Steuerelement schlägt fehl, wenn es IPSet keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `aws:` beginnen, werden ignoriert.

Ein Tag (Markierung) ist eine Markierung, die Sie einer AWS -Ressource zuordnen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Tags können Ihnen helfen, -Ressourcen zu identifizieren, Tags können Ihnen helfen, -Ressourcen zu identifizieren, um -Ressourcen zu identifizieren, um -Ressourcen zu identifizieren. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, die Berechtigungen basierend auf Tags definiert. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an AWS -Ressourcen anfügen. Sie können eine einzelne ABAC-Richtlinie oder einen separaten Richtlinienatz für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen zugelassen werden, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Was ist ABAC für AWS?](#) im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbare Informationen (PII) oder andere vertrauliche Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, einschließlich

AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der Allgemeinen AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem GuardDuty IPSets finden Sie [TagResource](#) in der Amazon GuardDuty API-Referenz.

[GuardDuty.4] GuardDuty Detektoren sollten markiert werden

Kategorie: Identifizieren > Inventar > Kennzeichnung

Schweregrad: Niedrig

Art der Ressource: `AWS::GuardDuty::Detector`

AWS Config Regel: `tagged-guardduty-detector` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Allowed Werte	Security Hub: Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Diese Steuerung prüft, ob ein GuardDuty Amazon-Detektor Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind `requiredTagKeys`. Die Steuerung schlägt fehl, wenn der Detektor keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft die Steuerung nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Detektor mit

keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag (Markierung) ist eine Markierung, die Sie einer AWS -Ressource zuordnen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Tags können Ihnen helfen, -Ressourcen zu identifizieren, Tags können Ihnen helfen, -Ressourcen zu identifizieren, um -Ressourcen zu identifizieren, um -Ressourcen zu identifizieren Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, die Berechtigungen basierend auf Tags definiert. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an AWS -Ressourcen anfügen. Sie können eine einzelne ABAC-Richtlinie oder einen separaten Richtlinienatz für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen zugelassen werden, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Was ist ABAC für AWS?](#) im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbare Informationen (PII) oder andere vertrauliche Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, einschließlich AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem GuardDuty Detektor finden Sie [TagResource](#) in der Amazon GuardDuty API-Referenz.

[GuardDuty.5] GuardDuty EKS Audit Log Monitoring sollte aktiviert sein

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Hoch

Ressourcentyp: `AWS::GuardDuty::Detector`

AWS Config -Regel: [guardduty-eks-protection-audit-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob GuardDuty EKS Audit Log Monitoring aktiviert ist. Bei einem eigenständigen Konto schlägt die Steuerung fehl, wenn GuardDuty EKS Audit Log Monitoring im Konto deaktiviert ist. In einer Umgebung mit mehreren Konten schlägt die Steuerung fehl, wenn für das delegierte GuardDuty Administratorkonto und alle Mitgliedskonten EKS Audit Log Monitoring nicht aktiviert ist.

In einer Umgebung mit mehreren Konten generiert das Control Ergebnisse nur für das delegierte GuardDuty Administratorkonto. Nur der delegierte Administrator kann die EKS-Audit-Protokoll-Überwachung für die Mitgliedskonten aktivieren oder deaktivieren. GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Diese Kontrolle generiert FAILED Ergebnisse, wenn der delegierte GuardDuty Administrator ein gesperrtes Mitgliedskonto hat, für das GuardDuty EKS Audit Log Monitoring nicht aktiviert ist. Um ein PASSED Ergebnis zu erhalten, muss der delegierte Administrator die Zuordnung dieser gesperrten Konten in aufheben. GuardDuty

GuardDuty EKS Audit Log Monitoring hilft Ihnen dabei, potenziell verdächtige Aktivitäten in Ihren Amazon Elastic Kubernetes Service (Amazon EKS) -Clustern zu erkennen. EKS Audit Log Monitoring verwendet Kubernetes-Prüfungsprotokolle, um chronologische Aktivitäten von Benutzern, Anwendungen, die die Kubernetes-API verwenden und der Steuerebene zu erfassen.

Abhilfe

Informationen zur Aktivierung von GuardDuty EKS Audit Log Monitoring finden Sie unter [EKS Audit Log Monitoring](#) im GuardDuty Amazon-Benutzerhandbuch.

[GuardDuty.6] GuardDuty Lambda Protection sollte aktiviert sein

Verwandte Anforderungen: PCI DSS v4.0.1/11.5.1

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Hoch

Art der Ressource: AWS::GuardDuty::Detector

AWS Config -Regel: [guardduty-lambda-protection-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob GuardDuty Lambda Protection aktiviert ist. Bei einem eigenständigen Konto schlägt die Steuerung fehl, wenn GuardDuty Lambda Protection im Konto deaktiviert ist. In einer Umgebung mit mehreren Konten schlägt die Steuerung fehl, wenn für das delegierte GuardDuty Administratorkonto und alle Mitgliedskonten Lambda Protection nicht aktiviert ist.

In einer Umgebung mit mehreren Konten generiert das Control Ergebnisse nur für das delegierte GuardDuty Administratorkonto. Nur der delegierte Administrator kann die Lambda Protection-Funktion für die Mitgliedskonten in der Organisation aktivieren oder deaktivieren. GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Dieses Steuerelement generiert FAILED Ergebnisse, wenn der delegierte GuardDuty Administrator über ein gesperrtes Mitgliedskonto verfügt, für das GuardDuty Lambda Protection nicht aktiviert ist. Um ein PASSED Ergebnis zu erhalten, muss der delegierte Administrator die Zuordnung dieser gesperrten Konten in aufheben. GuardDuty

GuardDuty Lambda Protection hilft Ihnen, potenzielle Sicherheitsbedrohungen zu identifizieren, wenn eine AWS Lambda -Funktion aufgerufen wird. Nachdem Sie Lambda Protection aktiviert haben, GuardDuty beginnt die Überwachung der Lambda-Netzwerkaktivitätsprotokolle, die mit den Lambda-Funktionen in Ihrem verknüpft sind. AWS-Konto Wenn eine Lambda-Funktion aufgerufen wird, der verdächtigen Netzwerkverkehr GuardDuty identifiziert, der auf das Vorhandensein eines potenziell bösartigen Codes in Ihrer Lambda-Funktion hindeutet, GuardDuty generiert dies eine Erkenntnis.

Abhilfe

Informationen zur Aktivierung von GuardDuty Lambda Protection finden Sie unter [Konfiguration des Lambda-Schutzes](#) im GuardDuty Amazon-Benutzerhandbuch.

[GuardDuty.7] GuardDuty EKS Runtime Monitoring sollte aktiviert sein

Verwandte Anforderungen: PCI DSS v4.0.1/11.5.1

Kategorie: Erkennen > Erkennungsdienste

Schweregrad: Mittel

Art der Ressource: AWS::GuardDuty::Detector

AWS Config -Regel: [guardduty-eks-protection-runtime-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob GuardDuty EKS Runtime Monitoring mit automatisierter Agentenverwaltung aktiviert ist. Bei einem eigenständigen Konto schlägt die Steuerung fehl, wenn GuardDuty EKS Runtime Monitoring mit automatisierter Agentenverwaltung im Konto deaktiviert ist. In einer Umgebung mit mehreren Konten schlägt die Steuerung fehl, wenn für das delegierte GuardDuty Administratorkonto und alle Mitgliedskonten EKS Runtime Monitoring mit automatisierter Agentenverwaltung nicht aktiviert ist.

In einer Umgebung mit mehreren Konten generiert das Control Ergebnisse nur für das delegierte GuardDuty Administratorkonto. Nur der delegierte Administrator kann die EKS-Runtime Monitoring-Funktion mit automatisierter Agentenverwaltung für die Mitgliedskonten in der Organisation aktivieren oder deaktivieren. GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Dieses Steuerelement generiert FAILED Ergebnisse, wenn der delegierte GuardDuty Administrator ein gesperrtes Mitgliedskonto hat, für das GuardDuty EKS Runtime Monitoring nicht aktiviert ist. Um ein PASSED Ergebnis zu erhalten, muss der delegierte Administrator die Zuordnung dieser gesperrten Konten in aufheben. GuardDuty

EKS Protection in Amazon GuardDuty bietet Bedrohungserkennung, um Sie beim Schutz von Amazon-EKS-Clustern in Ihrer AWS -Umgebung zu unterstützen. EKS-Laufzeit-Überwachung verwendet Ereignisse auf Betriebssystemebene, um Sie bei der Erkennung potenzieller Bedrohungen in EKS-Knoten und Containern innerhalb Ihrer EKS-Cluster zu unterstützen.

Abhilfe

Informationen zur Aktivierung von EKS Runtime Monitoring mit automatisierter Agentenverwaltung finden Sie unter [GuardDuty Enabling Runtime Monitoring](#) im GuardDuty Amazon-Benutzerhandbuch.

[GuardDuty.8] Der GuardDuty Malware-Schutz für EC2 sollte aktiviert sein

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Hoch

Ressourcentyp: AWS::GuardDuty::Detector

AWS Config -Regel: [guardduty-malware-protection-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob der GuardDuty Malware-Schutz aktiviert ist. Bei einem eigenständigen Konto schlägt die Steuerung fehl, wenn der GuardDuty Malware-Schutz im Konto deaktiviert ist. In einer Umgebung mit mehreren Konten schlägt die Steuerung fehl, wenn für das delegierte GuardDuty Administratorkonto und alle Mitgliedskonten der Malware-Schutz nicht aktiviert ist.

In einer Umgebung mit mehreren Konten generiert das Control Ergebnisse nur für das delegierte GuardDuty Administratorkonto. Nur der delegierte Administrator kann die Malware-Schutzfunktion für die Mitgliedskonten in der Organisation aktivieren oder deaktivieren. GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Diese Kontrolle generiert FAILED Ergebnisse, wenn der delegierte GuardDuty Administrator ein gesperrtes Mitgliedskonto hat, für das der GuardDuty Malware-Schutz nicht aktiviert ist. Um ein PASSED Ergebnis zu erhalten, muss der delegierte Administrator die Zuordnung dieser gesperrten Konten in aufheben. GuardDuty

GuardDuty Malware Protection for EC2 hilft Ihnen, das potenzielle Vorhandensein von Malware zu erkennen, indem es die Amazon Elastic Block Store (Amazon EBS) -Volumes scannt, die an Amazon Elastic Compute Cloud (Amazon EC2) -Instances und Container-Workloads angefügt sind. Malware Protection bietet Scan-Optionen, mit denen Sie entscheiden können, ob Sie bestimmte EC2 Instances und Container-Workloads beim Scannen ein- oder ausschließen möchten. Die Funktion bietet auch die Möglichkeit, die Snapshots der EBS-Volumes, die den EC2 Instances oder Container-Workloads zugeordnet sind, in Ihren Konten aufzubewahren. GuardDuty Die Snapshots werden nur aufbewahrt, wenn Malware gefunden wird und die Erkenntnisse von Malware Protection generiert werden.

Abhilfe

Informationen zur Aktivierung des GuardDuty Malware-Schutzes für EC2 finden Sie unter [Konfiguration des GuardDuty -initiierten Malware-Scans](#) im GuardDuty Amazon-Benutzerhandbuch.

[GuardDuty.9] Der GuardDuty RDS-Schutz sollte aktiviert sein

Verwandte Anforderungen: PCI DSS v4.0.1/11.5.1

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Hoch

Art der Ressource: AWS::GuardDuty::Detector

AWS Config -Regel: [guardduty-rds-protection-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob der GuardDuty RDS-Schutz aktiviert ist. Bei einem eigenständigen Konto schlägt die Steuerung fehl, wenn der GuardDuty RDS-Schutz im Konto deaktiviert ist. In einer Umgebung mit mehreren Konten schlägt die Steuerung fehl, wenn für das delegierte GuardDuty Administratorkonto und alle Mitgliedskonten der RDS-Schutz nicht aktiviert ist.

In einer Umgebung mit mehreren Konten generiert das Control Ergebnisse nur für das delegierte GuardDuty Administratorkonto. Nur der delegierte Administrator kann die Funktion RDS Protection für die Mitgliedskonten aktivieren oder deaktivieren. GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Dieses Steuerelement generiert FAILED Ergebnisse, wenn der delegierte GuardDuty Administrator ein gesperrtes Mitgliedskonto hat, für das der GuardDuty RDS-Schutz nicht aktiviert ist. Um ein PASSED Ergebnis zu erhalten, muss der delegierte Administrator die Zuordnung dieser gesperrten Konten in aufheben. GuardDuty

RDS Protection GuardDuty analysiert und profiliert RDS-Anmeldeaktivitäten im Hinblick auf potenzielle Zugriffsbedrohungen auf Ihre Amazon-Aurora-Datenbanken (Aurora MySQL-kompatible Edition und Aurora PostgreSQL-kompatible Edition). Mit dieses Feature können Sie potenziell verdächtiges Anmeldeverhalten identifizieren. RDS Protection erfordert keine zusätzliche Infrastruktur und ist so konzipiert, dass die Leistung Ihrer Datenbank-Instances nicht beeinträchtigt wird. Wenn es RDS Protection eine potenzielle Bedrohung erkennt, GuardDuty generiert das eine neue Erkenntnis mit Details zur potenziell kompromittierten Datenbank.

Abhilfe

Informationen zur Aktivierung des GuardDuty RDS-Schutzes finden Sie unter [GuardDuty RDS-Schutz](#) im GuardDuty Amazon-Benutzerhandbuch.

[GuardDuty.10] Der GuardDuty S3-Schutz sollte aktiviert sein

Verwandte Anforderungen: PCI DSS v4.0.1/11.5.1

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Hoch

Art der Ressource: AWS::GuardDuty::Detector

AWS Config -Regel: [guardduty-s3-protection-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob GuardDuty S3 Protection aktiviert ist. Bei einem eigenständigen Konto schlägt die Steuerung fehl, wenn GuardDuty S3 Protection im Konto deaktiviert ist. In einer Umgebung mit mehreren Konten schlägt die Steuerung fehl, wenn für das delegierte GuardDuty Administratorkonto und alle Mitgliedskonten S3 Protection nicht aktiviert ist.

In einer Umgebung mit mehreren Konten generiert das Control Ergebnisse nur für das delegierte GuardDuty Administratorkonto. Nur der delegierte Administrator kann die S3-Schutzfunktion für die Mitgliedskonten in der Organisation aktivieren oder deaktivieren. GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Diese Kontrolle generiert FAILED Ergebnisse, wenn der delegierte GuardDuty Administrator ein gesperrtes Mitgliedskonto hat, für das der GuardDuty S3-Schutz nicht aktiviert ist. Um ein PASSED Ergebnis zu erhalten, muss der delegierte Administrator die Zuordnung dieser gesperrten Konten in aufheben. GuardDuty

S3 Protection ermöglicht GuardDuty die Überwachung von API-Operationen auf Objektebene, um potenzielle Sicherheitsrisiken für Daten in Ihren Amazon-S3-Buckets zu identifizieren. GuardDuty überwacht Bedrohungen für Ihre S3-Ressourcen, indem AWS CloudTrail Verwaltungsereignisse und CloudTrail S3-Datenereignisse analysiert werden.

Abhilfe

Informationen zur Aktivierung von GuardDuty S3 Protection finden Sie unter [Amazon S3 Protection GuardDuty in Amazon](#) im GuardDuty Amazon-Benutzerhandbuch.

[GuardDuty.11] GuardDuty Runtime Monitoring sollte aktiviert sein

Kategorie: Erkennen > Erkennungsdienste

Schweregrad: Hoch

Art der Ressource: AWS::GuardDuty::Detector

AWS Config -Regel: [guardduty-runtime-monitoring-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob Runtime Monitoring in Amazon aktiviert ist GuardDuty. Bei einem eigenständigen Konto schlägt die Steuerung fehl, wenn GuardDuty Runtime Monitoring für das Konto

deaktiviert ist. In einer Umgebung mit mehreren Konten schlägt die Steuerung fehl, wenn GuardDuty Runtime Monitoring für das delegierte GuardDuty Administratorkonto und alle Mitgliedskonten deaktiviert ist.

In einer Umgebung mit mehreren Konten kann nur der delegierte GuardDuty Administrator die GuardDuty Laufzeit-Überwachung für Konten in seiner Organisation aktivieren oder deaktivieren. Darüber hinaus kann nur der GuardDuty Administrator die Security Agents konfigurieren und verwalten, die für die Laufzeitüberwachung von AWS Workloads und Ressourcen für Konten in der Organisation GuardDuty verwendet werden. GuardDuty Mitgliedskonten können Runtime Monitoring nicht für ihre eigenen Konten aktivieren, konfigurieren oder deaktivieren.

GuardDuty Laufzeit-Überwachung überwacht und analysiert Ereignisse auf Betriebssystemebene, Netzwerk und Dateiereignisse, um Sie bei der Erkennung potenzieller Bedrohungen in bestimmten AWS Workloads in Ihrer Umgebung zu unterstützen. Die GuardDuty Security Agents verwenden Security Agents, die das Laufzeitverhalten transparent machen, z. B. Dateizugriff, Prozessausführung, Befehlszeilenargumente und Netzwerkverbindungen. Sie können den Security Agent für jeden Ressourcentyp aktivieren und verwalten, den Sie auf potenzielle Bedrohungen überwachen möchten, z. B. Amazon EKS-Cluster und EC2 Amazon-Instances.

Abhilfe

Informationen zur Konfiguration und Aktivierung von GuardDuty Runtime Monitoring finden Sie unter [GuardDuty Runtime Monitoring](#) and [Enabling GuardDuty Runtime Monitoring](#) im GuardDuty Amazon-Benutzerhandbuch.

[GuardDuty.12] GuardDuty ECS Runtime Monitoring sollte aktiviert sein

Kategorie: Erkennen > Erkennungsdienste

Schweregrad: Mittel

Art der Ressource: AWS::GuardDuty::Detector

AWS Config -Regel: [guardduty-ecs-protection-runtime-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob der Amazon GuardDuty Automated Security Agent für die Laufzeitüberwachung von Amazon ECS-Clustern aktiviert ist AWS Fargate. Bei einem

eigenständigen Konto schlägt die Kontrolle fehl, wenn der Security Agent für das Konto deaktiviert ist. In einer Umgebung mit mehreren Konten schlägt die Steuerung fehl, wenn der Security Agent für das delegierte GuardDuty Administratorkonto und alle Mitgliedskonten deaktiviert ist.

In einer Umgebung mit mehreren Konten generiert diese Kontrolle Ergebnisse nur im delegierten GuardDuty Administratorkonto. Dies liegt daran, dass nur der delegierte GuardDuty Administrator die Laufzeitüberwachung von ECS-Fargate-Ressourcen für Konten in seiner Organisation aktivieren oder deaktivieren kann. GuardDuty Mitgliedskonten können dies nicht für ihre eigenen Konten tun. Darüber hinaus generiert diese Kontrolle FAILED Ergebnisse, wenn sie für ein Mitgliedskonto gesperrt GuardDuty ist und die Laufzeitüberwachung der ECS-Fargate-Ressourcen für das Mitgliedskonto deaktiviert ist. Um einen PASSED Befund zu erhalten, muss der GuardDuty Administrator das gesperrte Mitgliedskonto mit dem folgenden Befehl von seinem Administratorkonto trennen.

GuardDuty

GuardDuty Laufzeit-Überwachung überwacht und analysiert Ereignisse auf Betriebssystemebene, Netzwerk und Dateiereignisse, um Sie bei der Erkennung potenzieller Bedrohungen in bestimmten AWS Workloads in Ihrer Umgebung zu unterstützen. Die GuardDuty Security Agents verwenden Security Agents, die das Laufzeitverhalten transparent machen, z. B. Dateizugriff, Prozessausführung, Befehlszeilenargumente und Netzwerkverbindungen. Sie können den Security Agent für jeden Ressourcentyp aktivieren und verwalten, den Sie auf potenzielle Bedrohungen hin überwachen möchten. Dazu gehören Amazon ECS-Cluster auf AWS Fargate.

Abhilfe

Um den Security Agent für die GuardDuty Laufzeitüberwachung von ECS-Fargate-Ressourcen zu aktivieren und zu verwalten, müssen Sie ihn direkt verwenden. GuardDuty Sie können es nicht manuell für ECS-Fargate-Ressourcen aktivieren oder verwalten. Informationen zur Aktivierung und Verwaltung des Security Agents finden Sie unter [Voraussetzungen für den Support AWS Fargate \(nur Amazon ECS\)](#) und [Verwaltung des automatisierten Security Agents für AWS Fargate \(nur Amazon ECS\)](#) im GuardDuty Amazon-Benutzerhandbuch.

[GuardDuty.13] GuardDuty EC2 Runtime Monitoring sollte aktiviert sein

Kategorie: Erkennen > Erkennungsdienste

Schweregrad: Mittel

Art der Ressource: AWS::GuardDuty::Detector

AWS Config -Regel: [guardduty-ec2-protection-runtime-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob der Amazon GuardDuty Automated Security Agent für die Laufzeitüberwachung von EC2 Amazon-Instances aktiviert ist. Bei einem eigenständigen Konto schlägt die Kontrolle fehl, wenn der Security Agent für das Konto deaktiviert ist. In einer Umgebung mit mehreren Konten schlägt die Steuerung fehl, wenn der Security Agent für das delegierte GuardDuty Administratorkonto und alle Mitgliedskonten deaktiviert ist.

In einer Umgebung mit mehreren Konten generiert diese Kontrolle Ergebnisse nur im delegierten GuardDuty Administratorkonto. Dies liegt daran, dass nur der delegierte GuardDuty Administrator die Laufzeitüberwachung von EC2 Amazon-Instances für Konten in seiner Organisation aktivieren oder deaktivieren kann. GuardDuty Mitgliedskonten können dies nicht für ihre eigenen Konten tun. Darüber hinaus generiert dieses Steuerelement FAILED Ergebnisse, wenn GuardDuty es für ein Mitgliedskonto gesperrt ist und die Laufzeitüberwachung von EC2 Instanzen für das Mitgliedskonto deaktiviert ist. Um einen PASSED Befund zu erhalten, muss der GuardDuty Administrator das gesperrte Mitgliedskonto mit GuardDuty dem folgenden Befehl von seinem Administratorkonto trennen.

GuardDuty Laufzeit-Überwachung überwacht und analysiert Ereignisse auf Betriebssystemebene, Netzwerk und Dateiereignisse, um Sie bei der Erkennung potenzieller Bedrohungen in bestimmten AWS Workloads in Ihrer Umgebung zu unterstützen. Es verwendet GuardDuty Sicherheitsagenten, die das Laufzeitverhalten transparent machen, z. B. Dateizugriff, Prozessausführung, Befehlszeilenargumente und Netzwerkverbindungen. Sie können den Security Agent für jeden Ressourcentyp aktivieren und verwalten, den Sie auf potenzielle Bedrohungen hin überwachen möchten. Dies schließt EC2 Amazon-Instances ein.

Abhilfe

Informationen zur Konfiguration und Verwaltung des automatisierten Security Agents für die GuardDuty Laufzeitüberwachung von EC2 Instances finden Sie unter [Voraussetzungen für die Unterstützung von EC2 Amazon-Instances](#) und [Aktivieren des automatisierten Security Agents für EC2 Amazon-Instances](#) im GuardDuty Amazon-Benutzerhandbuch.

Security Hub-Steuerungen für AWS Identity and Access Management

Diese AWS Security Hub Kontrollen bewerten den AWS Identity and Access Management (IAM-) Dienst und die Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[IAM.1] IAM-Richtlinien sollten keine vollen „*“-Administratorrechte zulassen

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/1.22, CIS AWS Foundations Benchmark v1.4.0/1.16,, NIST.800-53.r5 AC-2 (1), (15) NIST.800-53.r5 AC-2, (7),,, (10) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (2), NIST.800-53.r5 AC-3 (3), NIST.800-171.r2 3.1.4 NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 PCI DSS v3.2.1/7.2.1 NIST.800-53.r5 AC-6 NIST.800-53.r5 AC-6

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Hoch

Art der Ressource: AWS::IAM::Policy

AWS Config -Regel: [iam-policy-no-statements-with-admin-access](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `excludePermissionBoundaryPolicy: true`(nicht anpassbar)

Dieses Steuerelement überprüft, ob die Standardversion der IAM-Richtlinien (auch als vom Kunden verwaltete Richtlinien bezeichnet) Administratorzugriff hat. Dazu wird eine Erklärung mit dem Zusatz „`Effect`: `Allow`“ mit `Action`: `*` über `Resource`: `*`“ hinzugefügt. Die Kontrolle schlägt fehl, wenn Sie über IAM-Richtlinien mit einer solchen Erklärung verfügen.

Das Steuerelement prüft nur die vom Kunden verwalteten Richtlinien, die Sie erstellen. Inline-Richtlinien und AWS verwaltete Richtlinien werden nicht geprüft.

IAM-Richtlinien definieren eine Reihe von Rechten, die Benutzern, Gruppen oder Rollen gewährt werden. Gemäß den üblichen Sicherheitshinweisen wird AWS empfohlen, die geringsten Rechte zu gewähren, d. h., nur die Berechtigungen zu gewähren, die für die Ausführung einer Aufgabe erforderlich sind. Wenn Sie umfassende administrative Berechtigungen anstelle nur derjenigen bereitstellen, die der Benutzer für seine Tätigkeit benötigt, ermöglichen Sie unter Umständen ungewollte Aktionen mit den Ressourcen.

Anstatt umfassende administrative Berechtigungen zu gewähren, legen Sie fest, was Benutzer tun müssen, und erstellen Sie dann Richtlinien, mit denen die Benutzer nur diese Aufgaben ausführen können. Es ist sicherer, mit einem Mindestsatz von Berechtigungen zu beginnen und bei Bedarf

zusätzliche Berechtigungen zu erteilen. Beginnen Sie nicht mit Berechtigungen, die zu weit gefasst sind, und versuchen Sie dann, sie später zu begrenzen.

Sie sollten IAM-Richtlinien entfernen, die eine Erklärung "Effect": "Allow" mit der Aufschrift "Action": "*" über "Resource": "*" enthalten.

 Note

AWS Config sollte in allen Regionen aktiviert sein, in denen Sie Security Hub verwenden. Die globale Ressourcenaufzeichnung kann jedoch in einer einzigen Region aktiviert werden. Wenn Sie nur globale Ressourcen in einer einzelnen Region erfassen, können Sie diese Kontrolle in allen Regionen mit Ausnahme der Region deaktivieren, in der Sie globale Ressourcen aufzeichnen.

Abhilfe

Informationen dazu, wie Sie Ihre IAM-Richtlinien so ändern, dass sie keine vollen „*“ - Administratorrechte gewähren, finden Sie unter [Bearbeiten von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

[IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/1.15, CIS AWS Foundations Benchmark v1.2.0/1.16,, NIST.800-53.r5 AC-2 (1), (15), (7) NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-6 (3) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 NIST.800-171.r2 3.1.1, NIST.800-53.r5 AC-3 NIST.800-171.r2 3.1.2 NIST.800-53.r5 AC-6, NIST.800-171.R2 3.1.7, NIST.800-171.r2 3.3.9, NIST.800-171.r2 3.13.3, PCI DSS v3.2.1/7.2.1

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Niedrig

Art der Ressource: AWS::IAM::User

AWS Config -Regel: [iam-user-no-policies-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Ihren IAM-Benutzern Richtlinien zugeordnet sind. Die Kontrolle schlägt fehl, wenn Ihren IAM-Benutzern Richtlinien zugewiesen sind. Stattdessen müssen IAM-Benutzer Berechtigungen von IAM-Gruppen erben oder eine Rolle übernehmen.

Standardmäßig haben IAM-Benutzer, -Gruppen und -Rollen keinen Zugriff auf Ressourcen. AWS IAM-Richtlinien gewähren Benutzern, Gruppen oder Rollen Rechte. Wir empfehlen, dass Sie IAM-Richtlinien direkt auf Gruppen und Rollen anwenden, jedoch nicht auf Benutzer. Das Zuweisen von Berechtigungen auf Gruppen- oder Rollenebene reduziert die Komplexität bei der Zugriffsverwaltung, wenn die Benutzeranzahl steigt. Eine Reduzierung der Komplexität bei der Zugriffsverwaltung kann wiederum das Risiko mindern, dass ein Prinzipal irrtümlicherweise übermäßige Berechtigungen erhält.

Note

AWS Config sollte in allen Regionen aktiviert sein, in denen Sie Security Hub verwenden. Die globale Ressourcenaufzeichnung kann jedoch in einer einzigen Region aktiviert werden. Wenn Sie globale Ressourcen nur in einer einzigen Region aufzeichnen, können Sie diese Steuerung in allen Regionen außer der Region deaktivieren, in der Sie globale Ressourcen aufzeichnen.

Abhilfe

Um dieses Problem zu beheben, [erstellen Sie eine IAM-Gruppe](#) und hängen Sie die Richtlinie an die Gruppe an. [Fügen Sie dann die Benutzer der Gruppe hinzu](#). Die Richtlinie gilt für jeden Benutzer in der Gruppe. Informationen zum Entfernen einer direkt mit einem Benutzer verknüpften Richtlinie finden Sie unter [Hinzufügen und Entfernen von IAM-Identitätsberechtigungen](#) im IAM-Benutzerhandbuch.

[IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/1.14, CIS Foundations Benchmark v1.4.0/1.14, CIS AWS Foundations Benchmark v1.2.0/1.4, NIST.800-53.r5 AC-2 (1), (3), (15), PCI DSS v4.0.1/8.3.9, PCI DSS NIST.800-53.r5 AC-2 v4.0.1/8.6.3 AWS NIST.800-53.r5 AC-3

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: AWS::IAM::User

AWS Config -Regel: [access-keys-rotated](#)

Art des Zeitplans: Periodisch

Parameter:

- maxAccessKeyAge: 90 (nicht anpassbar)

Dieses Steuerelement prüft, ob die aktiven Zugriffsschlüssel innerhalb von 90 Tagen rotiert werden.

Wir empfehlen Ihnen dringend, nicht alle Zugriffsschlüssel in Ihrem Konto zu generieren und zu entfernen. Stattdessen empfiehlt es sich, entweder eine oder mehrere IAM-Rollen zu erstellen oder den [Verbund](#) über AWS IAM Identity Center zu verwenden. Sie können diese Methoden verwenden, um Ihren Benutzern den Zugriff auf AWS Management Console und AWS CLI zu ermöglichen.

Jeder Ansatz hat seine Anwendungsfälle. Ein Verbund eignet sich im Allgemeinen besser für Unternehmen, die bereits über ein zentrales Verzeichnis verfügen oder planen, mehr als das derzeitige Limit für IAM-Benutzer zu benötigen. Anwendungen, die außerhalb einer AWS Umgebung ausgeführt werden, benötigen Zugriffstasten für den programmatischen Zugriff AWS auf Ressourcen.

Wenn die Ressourcen, die programmatischen Zugriff benötigen, jedoch intern ausgeführt werden AWS, empfiehlt es sich, IAM-Rollen zu verwenden. Rollen ermöglichen es Ihnen, einer Ressource Zugriff zu gewähren, ohne eine Zugriffsschlüssel-ID und einen geheimen Zugriffsschlüssel in die Konfiguration zu integrieren.

Weitere Informationen zum Schutz Ihrer Zugriffsschlüssel und Ihres Kontos finden Sie unter [Bewährte Methoden für die Verwaltung von AWS Zugriffsschlüsseln](#) in der. Allgemeine AWS-Referenz Lesen Sie auch den Blogbeitrag [Richtlinien für Ihren Schutz AWS-Konto bei der Verwendung von programmatischem Zugriff](#).

Wenn Sie bereits über einen Zugriffsschlüssel verfügen, empfiehlt Security Hub, die Zugangsschlüssel alle 90 Tage zu wechseln. Das Rotieren von Zugriffsschlüsseln reduziert die Gefahr, dass ein Zugriffsschlüssel eines kompromittierten oder gesperrten Kontos verwendet werden kann. Außerdem wird sichergestellt, dass mit einem alten Schlüssel, der möglicherweise verloren gegangen ist, geknackt bzw. gestohlen wurde, nicht auf Daten zugegriffen werden kann. Aktualisieren Sie Ihre Anwendungen immer, nachdem Sie Zugriffsschlüssel rotiert haben.

Zugriffsschlüssel bestehen aus einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel. Sie werden verwendet, um programmatische Anfragen zu signieren, die Sie stellen AWS. Benutzer

benötigen ihre eigenen Zugriffstasten AWS CLI, um programmgesteuerte Aufrufe AWS über die Tools für Windows PowerShell oder direkte HTTP-Aufrufe mithilfe der AWS SDKs API-Operationen für einzelne Benutzer zu tätigen. AWS-Services

Wenn Ihre Organisation AWS IAM Identity Center (IAM Identity Center) verwendet, können sich Ihre Benutzer bei Active Directory, einem integrierten IAM Identity Center-Verzeichnis oder einem [anderen Identitätsanbieter \(IdP\) anmelden, der mit IAM Identity Center verbunden](#) ist. Sie können dann einer IAM-Rolle zugeordnet werden, die es ihnen ermöglicht, AWS CLI Befehle auszuführen oder AWS API-Operationen aufzurufen, ohne dass Zugriffsschlüssel erforderlich sind. Weitere Informationen finden Sie im AWS Command Line Interface Benutzerhandbuch [unter Konfiguration der AWS CLI zu AWS IAM Identity Center verwendenden](#).

 Note

AWS Config sollte in allen Regionen aktiviert sein, in denen Sie Security Hub verwenden. Die globale Ressourcenaufzeichnung kann jedoch in einer einzigen Region aktiviert werden. Wenn Sie nur globale Ressourcen in einer einzelnen Region erfassen, können Sie diese Kontrolle in allen Regionen mit Ausnahme der Region deaktivieren, in der Sie globale Ressourcen aufzeichnen.

Abhilfe

Informationen zur Rotation von Zugriffsschlüsseln, die älter als 90 Tage sind, finden Sie unter [Rotieren von Zugriffsschlüsseln](#) im IAM-Benutzerhandbuch. Folgen Sie den Anweisungen für alle Benutzer, deren Zugriffsschlüssel älter als 90 Tage ist.

[IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/1.4, CIS AWS Foundations Benchmark v1.4.0/1.4, CIS Foundations Benchmark v1.2.0/1.12, PCI DSS v3.2.1/2.1, PCI DSS v3.2.1/7.2.1, (1), (15), (7), (10), (2) AWS NIST.800-53.r5 AC-2 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6 NIST.800-53.r5 AC-6 NIST.800-53.r5 AC-6

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Kritisch

Art der Ressource: AWS:::Account

AWS Config -Regel: [iam-root-access-key-check](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob der Root-Benutzerzugriffsschlüssel vorhanden ist.

Der Root-Benutzer ist der Benutzer mit den meisten Rechten in einem AWS-Konto. AWS Zugriffstasten ermöglichen den programmatischen Zugriff auf ein bestimmtes Konto.

Security Hub empfiehlt, dass Sie alle Zugriffsschlüssel entfernen, die dem Root-Benutzer zugeordnet sind. Dies schränkt die Vektoren ein, die verwendet werden können, um Ihr Konto zu gefährden. Darüber hinaus fördert es die Erstellung und Verwendung rollenbasierter Konten nach dem Prinzip der minimalen Rechte.

Abhilfe

Informationen zum Löschen des Root-Benutzerzugriffsschlüssels finden Sie unter [Löschen von Zugriffsschlüsseln für den Root-Benutzer](#) im IAM-Benutzerhandbuch. Informationen zum Löschen der Root-Benutzerzugriffsschlüssel aus einem AWS-Konto IN AWS GovCloud (US) finden Sie unter [Löschen der Root-Benutzerzugriffsschlüssel für mein AWS GovCloud \(US\) Konto](#) im AWS GovCloud (US) Benutzerhandbuch.

[IAM.5] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/1.10, CIS AWS Foundations Benchmark v1.4.0/1.10, CIS AWS Foundations Benchmark v1.2.0/1.2, (1), (15), NIST.800-53.r5 AC-2 (1), (2), NIST.800-53.r5 AC-3 (6), NIST.800-53.r5 IA-2 (8), NIST.800-53.r5 IA-2 PCI DSS v4.0.1/8.4.2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: AWS::IAM::User

AWS Config -Regel: [mfa-enabled-for-iam-console-access](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob die AWS Multi-Faktor-Authentifizierung (MFA) für alle IAM-Benutzer aktiviert ist, die ein Konsolenkennwort verwenden.

Multi-Factor Authentication (MFA) bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Wenn MFA aktiviert ist, wird ein Benutzer, wenn er sich AWS auf einer Website anmeldet, nach seinem Benutzernamen und Passwort gefragt. Darüber hinaus werden sie von ihrem AWS MFA-Gerät zur Eingabe eines Authentifizierungscodes aufgefordert.

Es wird empfohlen, MFA für alle Konten zu aktivieren, die über ein Konsolenpasswort verfügen. MFA wurde entwickelt, um mehr Sicherheit für den Konsolenzugriff zu bieten. Der authentifizierende Prinzipal muss über ein Gerät verfügen, das einen zeitkritischen Schlüssel ausgibt und Kenntnisse über Anmeldeinformationen haben muss.

 Note

AWS Config sollte in allen Regionen aktiviert sein, in denen Sie Security Hub verwenden. Die globale Ressourcenaufzeichnung kann jedoch in einer einzigen Region aktiviert werden. Wenn Sie nur globale Ressourcen in einer einzelnen Region erfassen, können Sie diese Kontrolle in allen Regionen mit Ausnahme der Region deaktivieren, in der Sie globale Ressourcen aufzeichnen.

Abhilfe

Informationen zum Hinzufügen von MFA für IAM-Benutzer finden Sie unter [Verwenden der Multi-Faktor-Authentifizierung \(MFA\) AWS im IAM-Benutzerhandbuch](#).

Wir bieten berechtigten Kunden einen kostenlosen MFA-Sicherheitsschlüssel an. [Prüfen Sie, ob Sie sich qualifizieren, und bestellen Sie Ihren kostenlosen Schlüssel](#).

[IAM.6] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/1.6, CIS AWS Foundations Benchmark v1.4.0/1.6, CIS Foundations Benchmark v1.2.0/1.14, PCI DSS v3.2.1/8.3.1, (1), (15), NIST.800-53.r5 AC-2 (1), (2), (6), NIST.800-53.r5 AC-3 (8), PCI DSS v4.0.1/8.4.2 AWS NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Kritisch

Art der Ressource: AWS:::Account

AWS Config -Regel: [root-account-hardware-mfa-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement überprüft, ob Sie AWS-Konto für die Verwendung eines Hardware-Geräts mit Multi-Faktor-Authentifizierung (MFA) aktiviert sind, um sich mit Root-Benutzeranmeldedaten anzumelden. Die Steuerung schlägt fehl, wenn Hardware-MFA nicht aktiviert ist oder virtuelle MFA-Geräte sich mit Root-Benutzeranmeldedaten anmelden dürfen.

Eine virtuelle MFA bietet möglicherweise nicht das gleiche Sicherheitsniveau wie ein Hardware-MFA-Gerät. Wir empfehlen, dass Sie ein virtuelles MFA-Gerät nur verwenden, solange Sie auf die Genehmigung des Hardwarekaufs oder auf das Eintreffen Ihrer Hardware warten.

Weitere Informationen finden Sie unter [Zuweisen eines virtuellen MFA-Geräts \(Konsole\)](#) im IAM-Benutzerhandbuch.

Note

Security Hub bewertet diese Kontrolle anhand des Vorhandenseins von Root-Benutzeranmeldedaten (Anmeldeprofil) in einem AWS-Konto. Die Kontrolle generiert PASSED Ergebnisse in den folgenden Fällen:

- Root-Benutzeranmeldeinformationen sind im Konto vorhanden und Hardware-MFA ist für den Root-Benutzer aktiviert.
- Root-Benutzeranmeldedaten sind im Konto nicht vorhanden.

Das Steuerelement generiert einen FAILED Befund, wenn Root-Benutzeranmeldedaten im Konto vorhanden sind und Hardware-MFA für den Root-Benutzer nicht aktiviert ist.

Abhilfe

Informationen zur Aktivierung von Hardware-MFA für den Root-Benutzer finden Sie unter [Multi-Faktor-Authentifizierung für an Root-Benutzer des AWS-Kontos](#) im IAM-Benutzerhandbuch.

Wir bieten berechtigten Kunden einen kostenlosen MFA-Sicherheitsschlüssel an. Informationen darüber, ob Sie berechtigt sind, finden Sie im [MFA Security Key-Programm FAQs](#).

[IAM.7] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1), (3), (15), NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 NIST.800-171.R2 3.5.2, NIST.800-53.r5 IA-5 NIST.800-171.R2 3.5.7, NIST.800-171.R2 3.5.8, PCI DSS v4.0.1/8.3.6, PCI DSS v4.0.1/8.3.7, PCI DSS v4.0.1/8.3.9, PCI DSS v4.0.1/8.3.9, PCI DSS v4.0.1/8.3.9, PCI DSS v4.0.1/8.3.10.1 0,1/8,6,3

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: AWS:::Account

AWS Config -Regel: [iam-password-policy](#)

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
RequireUppercaseCharacters	Das Passwort muss mindestens einen Großbuchstaben enthalten	Boolesch	true oder false	true
RequireLowercaseCharacters	Das Passwort muss mindestens einen Kleinbuchstaben enthalten	Boolesch	true oder false	true
RequireSymbols	Das Passwort muss mindestens ein Symbol enthalten	Boolesch	true oder false	true
RequireNumbers	Das Passwort muss mindestens eine Zahl enthalten	Boolesch	true oder false	true

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
MinimumPasswordLength	Mindestanzahl von Zeichen im Passwort	Ganzzahl	8 auf 128	8
PasswordReusePrevention	Anzahl der Passwortrotationen , bevor ein altes Passwort wiederverwendet werden kann	Ganzzahl	12 auf 24	Kein Standardwert
MaxPasswordAge	Anzahl der Tage bis zum Ablauf des Passworts	Ganzzahl	1 auf 90	Kein Standardwert

Dieses Steuerelement prüft, ob die Kontopasswortrichtlinie für IAM-Benutzer starke Konfigurationen verwendet. Die Steuerung schlägt fehl, wenn die Kennwortrichtlinie keine starken Konfigurationen verwendet. Sofern Sie keine benutzerdefinierten Parameterwerte angeben, verwendet Security Hub die in der vorherigen Tabelle genannten Standardwerte. Die MaxPasswordAge Parameter PasswordReusePrevention und haben keinen Standardwert. Wenn Sie diese Parameter ausschließen, ignoriert Security Hub bei der Auswertung dieser Steuerung die Anzahl der Kennwortrotationen und das Kennwortalter.

Für den Zugriff auf AWS Management Console benötigen IAM-Benutzer Passwörter. Als bewährte Methode empfiehlt Security Hub dringend, anstelle der Erstellung von IAM-Benutzern den Verbund zu verwenden. Mit dem Verbund können sich Benutzer mit ihren vorhandenen Unternehmensanmeldeinformationen bei der AWS Management Console anmelden. Verwenden Sie AWS IAM Identity Center (IAM Identity Center), um den Benutzer zu erstellen oder zu verbinden, und übernehmen Sie dann eine IAM-Rolle für ein Konto.

Weitere Informationen zu Identitätsanbietern und Verbund finden Sie unter [Identitätsanbieter und Verbund](#) im IAM-Benutzerhandbuch. Weitere Informationen zu IAM Identity Center finden Sie im [AWS IAM Identity Center Benutzerhandbuch](#).

Wenn Sie IAM-Benutzer verwenden müssen, empfiehlt Security Hub, die Erstellung sicherer Benutzerkennwörter zu erzwingen. Sie können auf Ihrem Computer eine Passwortrichtlinie einrichten AWS-Konto , um die Komplexitätsanforderungen und die obligatorischen Rotationsperioden für

Passwörter festzulegen. Wenn Sie eine Kennwortrichtlinie erstellen oder ändern, werden die meisten Einstellungen der Kennwortrichtlinie durchgesetzt, wenn Benutzer ihre Passwörter das nächste Mal ändern. Einige Einstellungen werden sofort durchgesetzt.

Abhilfe

Informationen zur Aktualisierung Ihrer Kennwortrichtlinie finden Sie unter [Einrichten einer Kontokennwortrichtlinie für IAM-Benutzer](#) im IAM-Benutzerhandbuch.

[IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/1.3,, NIST.800-53.r5 AC-2 (1), (3) NIST.800-53.r5 AC-2, (15), NIST.800-53.r5 AC-3 (7),, NIST.800-53.r5 AC-2 NIST.800-171.R2 3.1.2 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 PCI DSS v3.2.1/8.1.4 NIST.800-53.r5 AC-6, PCI DSS v4.0.1/8.2.6

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: AWS::IAM::User

AWS Config -Regel: [iam-user-unused-credentials-check](#)

Art des Zeitplans: Periodisch

Parameter:

- `maxCredentialUsageAge`: 90 (nicht anpassbar)

Dieses Steuerelement prüft, ob Ihre IAM-Benutzer über Passwörter oder aktive Zugriffsschlüssel verfügen, die seit 90 Tagen nicht verwendet wurden.

IAM-Benutzer können mit verschiedenen Arten von Anmeldeinformationen wie Passwörtern oder Zugriffsschlüsseln auf AWS Ressourcen zugreifen.

Security Hub empfiehlt, alle Anmeldeinformationen zu entfernen oder zu deaktivieren, die 90 Tage oder länger nicht verwendet wurden. Durch das Deaktivieren oder Entfernen unnötiger Anmeldeinformationen reduzieren Sie den möglichen Schaden, der mit den Anmeldeinformationen eines kompromittierten oder ungenutzten Kontos angerichtet werden kann.

 Note

AWS Config sollte in allen Regionen aktiviert sein, in denen Sie Security Hub verwenden. Die globale Ressourcenaufzeichnung kann jedoch in einer einzigen Region aktiviert werden. Wenn Sie nur globale Ressourcen in einer einzelnen Region erfassen, können Sie diese Kontrolle in allen Regionen mit Ausnahme der Region deaktivieren, in der Sie globale Ressourcen aufzeichnen.

Abhilfe

Wenn Sie Benutzerinformationen in der IAM-Konsole anzeigen, gibt es Spalten für das Alter des Zugriffsschlüssels, das Alter des Kennworts und die letzte Aktivität. Wenn der Wert in einer dieser Spalten mehr als 90 Tage beträgt, sollten Sie die Anmeldeinformationen für diese Benutzer deaktivieren.

Sie können auch [Berichte mit Anmeldeinformationen](#) verwenden, um Benutzer zu überwachen und Benutzer zu identifizieren, die 90 oder mehr Tage lang keine Aktivität mehr hatten. Sie können Berichte über Anmeldeinformationen im .csv Format von der IAM-Konsole herunterladen.

Nachdem Sie die inaktiven Konten oder ungenutzten Anmeldeinformationen identifiziert haben, deaktivieren Sie sie. Anweisungen finden Sie im IAM-Benutzerhandbuch unter [Erstellen, Ändern oder Löschen eines IAM-Benutzerkennworts \(Konsole\)](#).

[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein

Verwandte Anforderungen: PCI DSS v3.2.1/8.3.1, PCI DSS v4.0.1/8.4.2, CIS Foundations Benchmark v3.0.0/1.5, CIS AWS Foundations Benchmark v1.4.0/1.5, CIS Foundations Benchmark v1.2.0/1.13, (1), (15), (1), (2), (AWS 6), (8) AWS NIST.800-53.r5 AC-2 NIST.800-53.r5 AC-3 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Kritisch

Art der Ressource: AWS:::Account

AWS Config -Regel: [root-account-mfa-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob die Multi-Faktor-Authentifizierung (MFA) aktiviert ist, damit sich der IAM-Root-Benutzer eines bei AWS-Konto dem anmelden kann. AWS Management Console Die Steuerung schlägt fehl, wenn MFA für den Root-Benutzer des Kontos nicht aktiviert ist.

Der IAM-Root-Benutzer von AWS-Konto hat vollständigen Zugriff auf alle Dienste und Ressourcen im Konto. Wenn MFA aktiviert ist, muss der Benutzer einen Benutzernamen, ein Passwort und einen Authentifizierungscode von seinem AWS MFA-Gerät eingeben, um sich bei dem anzumelden. AWS Management Console MFA fügt zusätzlich zu einem Benutzernamen und einem Passwort eine zusätzliche Schutzebene hinzu.

Diese Kontrolle generiert PASSED Ergebnisse in den folgenden Fällen:

- Root-Benutzeranmeldeinformationen sind im Konto vorhanden und MFA ist für den Root-Benutzer aktiviert.
- Root-Benutzeranmeldedaten sind im Konto nicht vorhanden.

Das Steuerelement generiert FAILED Ergebnisse, wenn Root-Benutzeranmeldeinformationen im Konto vorhanden sind und MFA für den Root-Benutzer nicht aktiviert ist.

Abhilfe

Informationen zur Aktivierung von MFA für den Root-Benutzer eines AWS-Konto finden Sie unter [Multi-Faktor-Authentifizierung für den Root-Benutzer des AWS-Kontos](#) im AWS Identity and Access Management Benutzerhandbuch.

[IAM.10] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein

Verwandte Anforderungen: NIST.800-171.R2 3.5.2, NIST.800-171.R2 3.5.7, NIST.800-171.r2 3.5.8, PCI DSS v3.2.1/8.1.4, PCI DSS v3.2.1/8.2.3, PCI DSS v3.2.1/8.2.4, PCI DSS v3.2.1/8.2.5

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Ressourcentyp: AWS :: Account

AWS Config -Regel: [iam-password-policy](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob die Kontopasswortrichtlinie für IAM-Benutzer die folgenden PCI-DSS-Mindestkonfigurationen verwendet.

- **RequireUppercaseCharacters**— Das Passwort muss mindestens einen Großbuchstaben enthalten. (Standardwert = `true`)
- **RequireLowercaseCharacters**— Das Passwort muss mindestens einen Kleinbuchstaben enthalten. (Standardwert = `true`)
- **RequireNumbers**— Erfordert mindestens eine Zahl im Passwort. (Standardwert = `true`)
- **MinimumPasswordLength**— Mindestlänge des Passworts. (Standard = 7 oder länger)
- **PasswordReusePrevention**— Anzahl der Passwörter vor der Wiederverwendung. (Standard = 4)
- **MaxPasswordAge**— Anzahl der Tage bis zum Ablauf des Passworts. (Standard = 90)

 Note

Am 30. Mai 2025 entfernte Security Hub dieses Steuerelement aus dem PCI DSS v4.0.1-Standard. PCI DSS v4.0.1 verlangt jetzt, dass Passwörter mindestens 8 Zeichen lang sind. Diese Steuerung gilt weiterhin für den Standard PCI DSS v3.2.1, für den andere Kennwortanforderungen gelten.

[Um die Kennwortrichtlinien für Konten anhand der Anforderungen von PCI DSS v4.0.1 zu bewerten, können Sie das IAM.7-Steuerelement verwenden.](#) Für dieses Steuerelement müssen Kennwörter mindestens 8 Zeichen lang sein. Es unterstützt auch benutzerdefinierte Werte für die Passwortlänge und andere Parameter. Die IAM.7-Steuerung ist Teil des PCI DSS v4.0.1-Standards in Security Hub.

Abhilfe

Informationen zur Aktualisierung Ihrer Kennwortrichtlinie zur Verwendung der empfohlenen Konfiguration finden Sie unter [Einrichten einer Kontokennwortrichtlinie für IAM-Benutzer im IAM-Benutzerhandbuch](#).

[IAM.11] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/1.5, NIST.800-171.R2 3.5.7, PCI DSS v4.0.1/8.3.6, PCI DSS v4.0.1/8.6.3

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: AWS:::Account

AWS Config -Regel: [iam-password-policy](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Passwortrichtlinien erzwingen zum Teil Anforderungen in Zusammenhang mit der Passwortkomplexität. Verwenden Sie IAM-Passwortrichtlinien, um sicherzustellen, dass Passwörter unterschiedliche Zeichensätze verwenden.

CIS empfiehlt, dass die Kennwortrichtlinie mindestens einen Großbuchstaben erfordert. Die Festlegung einer Richtlinie für die Passwortkomplexität steigert die Widerstandskraft eines Kontos gegen Brute-Force-Anmeldeversuche.

Abhilfe

Informationen zum Ändern Ihrer Kennwortrichtlinie finden Sie unter [Einrichten einer Kontokennwortrichtlinie für IAM-Benutzer](#) im IAM-Benutzerhandbuch. Wählen Sie unter Passwortstärke die Option Mindestens einen Großbuchstaben des lateinischen Alphabets erforderlich (A—Z) aus.

[IAM.12] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/1.6, NIST.800-171.R2 3.5.7, PCI DSS v4.0.1/8.3.6, PCI DSS v4.0.1/8.6.3

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: AWS:::Account

AWS Config -Regel: [iam-password-policy](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Passwortrichtlinien erzwingen zum Teil Anforderungen in Zusammenhang mit der Passwortkomplexität. Verwenden Sie IAM-Passwortrichtlinien, um sicherzustellen, dass Passwörter unterschiedliche Zeichensätze verwenden. CIS empfiehlt, dass die Kennwortrichtlinie mindestens einen Kleinbuchstaben erfordert. Die Festlegung einer Richtlinie für die Passwortkomplexität steigert die Widerstandskraft eines Kontos gegen Brute-Force-Anmeldeversuche.

Abhilfe

Informationen zum Ändern Ihrer Kennwortrichtlinie finden Sie unter [Einrichten einer Kontokennwortrichtlinie für IAM-Benutzer](#) im IAM-Benutzerhandbuch. Wählen Sie unter Passwortstärke die Option Mindestens einen Kleinbuchstaben aus dem lateinischen Alphabet erforderlich (A—Z) aus.

[IAM.13] Stellen Sie sicher, dass für die IAM-Passwortrichtlinie mindestens ein Symbol erforderlich ist

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/1.7, NIST.800-171.R2 3.5.7

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: AWS:::Account

AWS Config -Regel: [iam-password-policy](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Passwortrichtlinien erzwingen zum Teil Anforderungen in Zusammenhang mit der Passwortkomplexität. Verwenden Sie IAM-Passwortrichtlinien, um sicherzustellen, dass Passwörter unterschiedliche Zeichensätze verwenden.

CIS empfiehlt, dass für die Kennwortrichtlinie mindestens ein Symbol erforderlich ist. Die Festlegung einer Richtlinie für die Passwortkomplexität steigert die Widerstandskraft eines Kontos gegen Brute-Force-Anmeldeversuche.

Abhilfe

Informationen zum Ändern Ihrer Kennwortrichtlinie finden Sie unter [Einrichten einer Kontokennwortrichtlinie für IAM-Benutzer](#) im IAM-Benutzerhandbuch. Wählen Sie unter Passwortstärke die Option Mindestens ein nichtalphanumerisches Zeichen erforderlich aus.

[IAM.14] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/1.8, NIST.800-171.R2 3.5.7, PCI DSS v4.0.1/8.3.6, PCI DSS v4.0.1/8.6.3

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: AWS:::Account

AWS Config -Regel: [iam-password-policy](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Passwortrichtlinien erzwingen zum Teil Anforderungen in Zusammenhang mit der Passwortkomplexität. Verwenden Sie IAM-Passwortrichtlinien, um sicherzustellen, dass Passwörter unterschiedliche Zeichensätze verwenden.

CIS empfiehlt, dass die Kennwortrichtlinie mindestens eine Zahl erfordert. Die Festlegung einer Richtlinie für die Passwortkomplexität steigert die Widerstandskraft eines Kontos gegen Brute-Force-Anmeldeversuche.

Abhilfe

Informationen zum Ändern Ihrer Kennwortrichtlinie finden Sie unter [Einrichten einer Kontokennwortrichtlinie für IAM-Benutzer](#) im IAM-Benutzerhandbuch. Wählen Sie unter Passwortstärke die Option Mindestens eine Zahl erforderlich aus.

[IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/1.8, CIS Foundations Benchmark v1.4.0/1.8, CIS AWS Foundations Benchmark v1.2.0/1.9, NIST.800-171.R2 3.5.7 AWS

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: AWS:::Account

AWS Config -Regel: [iam-password-policy](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Passwortrichtlinien erzwingen zum Teil Anforderungen in Zusammenhang mit der Passwortkomplexität. Verwenden Sie IAM-Passwortrichtlinien, um sicherzustellen, dass Passwörter mindestens eine bestimmte Länge haben.

CIS empfiehlt, dass die Kennwortrichtlinie eine Mindestkennwortlänge von 14 Zeichen vorschreibt. Die Festlegung einer Richtlinie für die Passwortkomplexität steigert die Widerstandskraft eines Kontos gegen Brute-Force-Anmeldeversuche.

Abhilfe

Informationen zum Ändern Ihrer Kennwortrichtlinie finden Sie unter [Einrichten einer Kontokennwortrichtlinie für IAM-Benutzer](#) im IAM-Benutzerhandbuch. Geben Sie für die Mindestlänge des Kennworts eine **14** oder eine größere Zahl ein.

[IAM.16] Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/1.9, CIS Foundations Benchmark v1.4.0/1.9, CIS AWS Foundations Benchmark v1.2.0/1.10, NIST.800-171.R2 3.5.8, PCI DSS v4.0.1/8.3.7 AWS

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Niedrig

Art der Ressource: AWS:::Account

AWS Config -Regel: [iam-password-policy](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob die Anzahl der zu merkenden Passwörter auf 24 gesetzt ist. Die Steuerung schlägt fehl, wenn der Wert nicht 24 ist.

IAM-Passwortrichtlinien können die Wiederverwendung eines bestimmten Passworts durch denselben Benutzer verhindern.

CIS empfiehlt, dass die Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert. Das Verhindern der Wiederverwendung von Passwörtern steigert die Widerstandskraft eines Kontos gegen Brute-Force-Anmeldeversuche.

Abhilfe

Informationen zum Ändern Ihrer Kennwortrichtlinie finden Sie unter [Einrichten einer Kontokennwortrichtlinie für IAM-Benutzer](#) im IAM-Benutzerhandbuch. Geben Sie für „Wiederverwendung von Passwörtern verhindern“ ein. **24**

[IAM.17] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/1.11, PCI DSS v4.0.1/8.3.9, PCI DSS v4.0.1/8.3.10.1

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Niedrig

Art der Ressource: AWS:::Account

AWS Config -Regel: [iam-password-policy](#)

Art des Zeitplans: Periodisch

Parameter: Keine

IAM-Passwortrichtlinien können vorschreiben, dass Passwörter nach einer bestimmten Anzahl von Tagen ausgetauscht werden oder abgelaufen sind.

CIS empfiehlt, dass die Kennwortrichtlinie Passwörter nach 90 Tagen oder weniger abläuft. Das Reduzieren der Lebensdauer von Passwörtern steigert die Widerstandskraft eines Kontos gegen Brute-Force-Anmeldeversuche. Darüber hinaus ist es in folgenden Situationen hilfreich, wenn regelmäßige Passwortänderungen gefordert werden:

- Passwörter können ohne Ihr Wissen gestohlen oder kompromittiert werden. Dies kann durch eine Systemkompromittierung, eine Softwareschwachstelle oder eine interne Bedrohung erfolgen.

- Bestimmte Web-Filter oder Proxy-Server von Unternehmen und Behörden können Datenverkehr abfangen und erfassen, selbst wenn er verschlüsselt ist.
- Viele Menschen verwenden dasselbe Passwort für viele Systeme, z. B. für die Arbeit, E-Mails und den privaten Gebrauch.
- Auf kompromittierten Endbenutzer-Workstations kann ein Keylogger vorhanden sein.

Abhilfe

Informationen zum Ändern Ihrer Kennwortrichtlinie finden Sie unter [Einrichten einer Kontokennwortrichtlinie für IAM-Benutzer](#) im IAM-Benutzerhandbuch. Geben Sie für „Ablauf des Kennworts aktivieren“ eine kleinere **90** Zahl oder ein.

[IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS -Support

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/1.17, CIS Foundations Benchmark v1.4.0/1.17, CIS AWS Foundations Benchmark v1.2.0/1.20, NIST.800-171.r2 3.1.2, PCI DSS v4.0.1/12.10.3 AWS

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Niedrig

Art der Ressource: AWS:::Account

AWS Config -Regel: [iam-policy-in-use](#)

Art des Zeitplans: Periodisch

Parameter:

- policyARN: arn:*partition*:iam::aws:policy/AWSSupportAccess (nicht anpassbar)
- policyUsageType: ANY (nicht anpassbar)

AWS bietet ein Support-Center, das für die Benachrichtigung und Reaktion auf Vorfälle sowie für technischen Support und Kundendienst genutzt werden kann.

Erstellen Sie eine IAM-Rolle, damit autorisierte Benutzer Vorfälle mit AWS Support verwalten können. Durch die Implementierung von Least-Privilegien für die Zugriffskontrolle erfordert eine IAM-Rolle

eine entsprechende IAM-Richtlinie, die den Zugriff auf das Supportcenter ermöglicht, damit Vorfälle bearbeitet werden können. Support

 Note

AWS Config sollte in allen Regionen aktiviert sein, in denen Sie Security Hub verwenden. Die globale Ressourcenaufzeichnung kann jedoch in einer einzigen Region aktiviert werden. Wenn Sie nur globale Ressourcen in einer einzelnen Region erfassen, können Sie diese Kontrolle in allen Regionen mit Ausnahme der Region deaktivieren, in der Sie globale Ressourcen aufzeichnen.

Abhilfe

Um dieses Problem zu beheben, erstellen Sie eine Rolle, die es autorisierten Benutzern ermöglicht, Support Vorfälle zu verwalten.

Um die Rolle zu erstellen, die für Support den Zugriff verwendet werden soll

1. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
2. Wählen Sie im IAM-Navigationsbereich Rollen und anschließend Rolle erstellen aus.
3. Wählen Sie als Rollentyp die Option Andere AWS-Konto aus.
4. Geben Sie unter Konto-ID die AWS-Konto ID der AWS-Konto Person ein, der Sie Zugriff auf Ihre Ressourcen gewähren möchten.

Wenn sich die Benutzer oder Gruppen, die diese Rolle übernehmen, im selben Konto befinden, geben Sie die lokale Kontonummer ein.

 Note

Der Administrator des angegebenen Kontos kann die Berechtigung erteilen, diese Rolle für alle -Benutzer in diesem Konto zu übernehmen. Hierzu fügt der Administrator eine Richtlinie an den Benutzer oder eine Gruppe an, mit der die Berechtigung für die Aktion `sts:AssumeRole` gewährt wird. In dieser Richtlinie muss die Ressource der Rollen-ARN sein.

5. Wählen Sie Weiter: Berechtigungen aus.
6. Suchen Sie nach der verwalteten Richtlinie `AWSSupportAccess`.

7. Wählen Sie das Kontrollkästchen für die verwaltete AWSSupportAccess-Richtlinie aus.
8. Wählen Sie Weiter: Tags aus.
9. (Optional) Um der Rolle Metadaten hinzuzufügen, fügen Sie Tags als Schlüssel-Wert-Paare hinzu.

Weitere Informationen zur Verwendung von Tags in IAM finden Sie unter [Tagging von IAM-Benutzern und -Rollen](#) im IAM-Benutzerhandbuch.

10. Klicken Sie auf Next: Review (Weiter: Prüfen).
11. Geben Sie unter Role name (Rollenname) einen Namen für Ihre Rolle ein.

Rollennamen müssen innerhalb Ihrer eindeutig sein. AWS-Konto Sie unterscheiden nicht zwischen Groß- und Kleinschreibung.

12. (Optional) Geben Sie im Feld Role description (Rollenbeschreibung) eine Beschreibung für die neue Rolle ein.
13. Prüfen Sie die Rolle und klicken Sie dann auf Create role (Rolle erstellen).

[IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1), (15), NIST.800-53.r5 AC-3 (1), NIST.800-53.r5 IA-2 (2), (6), NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 (8), NIST.800-53.r5 IA-2 NIST.800-171.R2 3.3.8, NIST.800-171.R2 3.5.3, NIST.800-171.r2 3.5.4, NIST.800-171.r2 3.7.5, PCI DSS v3.2.1/8.3.1, PCI DSS v4.0.1/8.4.2,

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Ressourcentyp: AWS : : IAM : : User

AWS Config -Regel: [iam-user-mfa-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob die IAM-Benutzer die Multi-Faktor-Authentifizierung (MFA) aktiviert haben.

 Note

AWS Config sollte in allen Regionen aktiviert sein, in denen Sie Security Hub verwenden. Die globale Ressourcenaufzeichnung kann jedoch in einer einzigen Region aktiviert werden. Wenn Sie nur globale Ressourcen in einer einzelnen Region erfassen, können Sie diese Kontrolle in allen Regionen mit Ausnahme der Region deaktivieren, in der Sie globale Ressourcen aufzeichnen.

Abhilfe

Informationen zum Hinzufügen von MFA für IAM-Benutzer finden Sie unter [Aktivieren von MFA-Geräten für Benutzer AWS im IAM-Benutzerhandbuch](#).

[IAM.20] Vermeiden Sie die Verwendung des Root-Benutzers

 Important

Security Hub hat diese Kontrolle im April 2024 eingestellt. Weitere Informationen finden Sie unter [Änderungsprotokoll für Security Hub CSPM-Steuerelemente](#).

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/1.1

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Niedrig

Art der Ressource: AWS::IAM::User

AWS Config Regel: use-of-root-account-test (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob für an AWS-Konto Beschränkungen für die Nutzung des Root-Benutzers gelten. Das Steuerelement bewertet die folgenden Ressourcen:

- Amazon Simple Notification Service (Amazon SNS)-Themen
- AWS CloudTrail Pfade

- Mit den CloudTrail Pfaden verknüpfte metrische Filter
- CloudWatch Amazon-Alarme basierend auf den Filtern

Bei dieser Prüfung wird FAILED festgestellt, ob eine oder mehrere der folgenden Aussagen zutreffen:

- Auf dem Konto sind keine CloudTrail Spuren vorhanden.
- Ein CloudTrail Trail ist aktiviert, aber nicht mit mindestens einem Trail für mehrere Regionen konfiguriert, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst.
- Ein CloudTrail Trail ist aktiviert, aber keiner CloudWatch Logs-Protokollgruppe zugeordnet.
- Der vom Center for Internet Security (CIS) vorgeschriebene exakte metrische Filter wird nicht verwendet. Der vorgeschriebene metrische Filter ist '\$.userIdentity.type="Root" && \$.userIdentity.invokedBy NOT EXISTS && \$.eventType != "AwsServiceEvent"'
- In dem Konto sind keine CloudWatch Alarme vorhanden, die auf dem metrischen Filter basieren.
- CloudWatch Alarme, die so konfiguriert sind, dass sie Benachrichtigungen an das zugehörige SNS-Thema senden, werden nicht aufgrund der Alarmbedingung ausgelöst.
- Das SNS-Thema entspricht nicht den [Einschränkungen für das Senden einer Nachricht an ein SNS-Thema](#).
- Das SNS-Thema hat nicht mindestens einen Abonnenten.

Diese Prüfung führt zu einem Kontrollstatus, der NO_DATA angibt, ob eine oder mehrere der folgenden Aussagen zutreffen:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

Diese Prüfung führt zu einem Kontrollstatus, der WARNING angibt, ob eine oder mehrere der folgenden Aussagen zutreffen:

- Das aktuelle Konto ist nicht Eigentümer des SNS-Themas, auf das in der CloudWatch Warnung verwiesen wird.
- Das Girokonto hat beim Aufrufen der SNS-API keinen Zugriff auf das SNS-Thema.
`ListSubscriptionsByTopic`

 Note

Wir empfehlen, Organization Trails zu verwenden, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von NO_DATA für Kontrollen, die in den Konten von Organisationsmitgliedern ausgewertet wurden. In Mitgliedskonten generiert Security Hub nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Es hat sich bewährt, Ihre Root-Benutzeranmeldedaten nur dann zu verwenden, wenn dies für die [Konto- und Serviceverwaltung](#) erforderlich ist. Wenden Sie IAM-Richtlinien direkt auf Gruppen und Rollen an, jedoch nicht auf Benutzer. Anweisungen zur Einrichtung eines Administrators für den täglichen Gebrauch finden Sie im [IAM-Benutzerhandbuch unter Erstellen Ihres ersten IAM-Admin-Benutzers und Ihrer ersten Gruppe](#).

Abhilfe

Die Schritte zur Behebung dieses Problems umfassen die Einrichtung eines Amazon SNS SNS-Themas, eines CloudTrail Trails, eines Metrikfilters und eines Alarms für den Metrikfilter.

Erstellen eines Amazon SNS-Themas

1. Öffnen Sie die Amazon SNS SNS-Konsole unter <https://console.aws.amazon.com/sns/v3/home>.
2. Erstellen Sie ein Amazon SNS SNS-Thema, das alle CIS-Alarme empfängt.

Erstellen Sie mindestens einen Abonnenten für das Thema. Weitere Informationen finden Sie unter [Erste Schritte mit Amazon SNS](#) im Benutzerhandbuch für Amazon Simple Notification Service.

Richten Sie als Nächstes eine aktive Option ein CloudTrail , die für alle Regionen gilt. Um dies zu tun, befolgen Sie die Schritte in [the section called “\[CloudTrail.1\] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst”](#).

Notieren Sie sich den Namen der Protokollgruppe CloudWatch Logs, die Sie dem CloudTrail Trail zuordnen. Sie erstellen den Metrikfilter für diese Protokollgruppe.

Erstellen Sie abschließend den metrischen Filter und den Alarm.

Erstellen eines Metrikfilters und Alarms

1. Öffnen Sie die CloudWatch Konsole unter <https://console.aws.amazon.com/cloudwatch/>.
2. Wählen Sie im Navigationsbereich Protokollgruppen aus.
3. Aktivieren Sie das Kontrollkästchen für die Protokollgruppe CloudWatch Logs, die dem von Ihnen erstellten CloudTrail Trail zugeordnet ist.
4. Wählen Sie unter Aktionen die Option Metrikfilter erstellen aus.
5. Gehen Sie unter Muster definieren wie folgt vor:
 - a. Kopieren Sie das folgende Muster und fügen Sie es dann in das Feld Filter Pattern (Filtermuster) ein.

```
{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType != "AwsServiceEvent"}
```

- b. Wählen Sie Weiter aus.
6. Gehen Sie unter Metrik zuweisen wie folgt vor:
 - a. Geben Sie im Feld Filtername einen Namen für Ihren Metrikfilter ein.
 - b. Geben **LogMetrics** Sie für Metric Namespace den Wert ein.

Wenn Sie denselben Namespace für alle Ihre CIS-Log-Metrikfilter verwenden, werden alle CIS-Benchmark-Metriken zusammen gruppiert.

- c. Geben Sie unter Metrikname einen Namen für die Metrik ein. Merken Sie sich den Namen der Metrik. Sie müssen die Metrik auswählen, wenn Sie den Alarm erstellen.
 - d. Geben Sie für Metric value (Metrikwert) **1** ein.
 - e. Wählen Sie Weiter aus.
7. Überprüfen Sie unter Überprüfen und erstellen die Informationen, die Sie für den neuen Metrikfilter angegeben haben. Wählen Sie dann Metrikfilter erstellen aus.
 8. Wählen Sie im Navigationsbereich Protokollgruppen und dann den Filter aus, den Sie unter Metrikfilter erstellt haben.
 9. Aktivieren Sie das Kontrollkästchen für den Filter. Wählen Sie Alarm erstellen aus.

10. Gehen Sie unter Metrik und Bedingungen angeben wie folgt vor:
 - a. Wählen Sie unter Bedingungen für Schwellenwert die Option Statisch aus.
 - b. Wählen Sie unter Alarmbedingung definieren die Option Größer/Gleich aus.
 - c. Geben Sie unter Schwellenwert definieren den Wert ein. **1**
 - d. Wählen Sie Weiter aus.
11. Gehen Sie unter Aktionen konfigurieren wie folgt vor:
 - a. Wählen Sie unter Auslöser für den Alarmstatus die Option Bei Alarm aus.
 - b. Wählen Sie unter Select an SNS topic (SNS-Thema auswählen) die Option Select an existing SNS topic (Vorhandenes SNS-Thema auswählen) aus.
 - c. Geben Sie unter Benachrichtigung senden an den Namen des SNS-Themas ein, das Sie im vorherigen Verfahren erstellt haben.
 - d. Wählen Sie Weiter aus.
12. Geben Sie unter Namen und Beschreibung hinzufügen einen Namen und eine Beschreibung für den Alarm ein, z. B. **CIS-1.1-RootAccountUsage** Wählen Sie anschließend Weiter.
13. Überprüfen Sie unter Vorschau und Erstellung die Alarmkonfiguration. Wählen Sie anschließend Create alarm (Alarm erstellen) aus.

[IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen

Verwandte Anforderungen: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), (15), (7) NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (10), NIST.800-53.r5 AC-3 (2), NIST.800-53.r5 AC-6 (3) NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 NIST.800-171.R2 3.1.1, NIST.800-53.r5 AC-6 NIST.800-171.R2 3.1.2, NIST.800-171.R2 3.1.5, NIST.800-171.R2 3.1.7, NIST.800-171.r2 3.3.8, NIST.800-171.r2 3.3.9, NIST.800-171.r2 3.3.9, NIST.800-171.r2 3.3.8 171.R2 3.13.3, NIST.800-171.R2 3.13.4

Kategorie: Erkennen > Sicheres Zugriffsmanagement

Schweregrad: Niedrig

Art der Ressource: AWS::IAM::Policy

AWS Config -Regel: [iam-policy-no-statements-with-full-access](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `excludePermissionBoundaryPolicy`: True (nicht anpassbar)

Dieses Steuerelement prüft, ob die identitätsbasierten IAM-Richtlinien, die Sie erstellen, über Allow-Anweisungen verfügen, die den Platzhalter „*“ verwenden, um Berechtigungen für alle Aktionen in einem Dienst zu gewähren. Das Steuerelement schlägt fehl, wenn eine Richtlinienanweisung mit enthält. `"Effect": "Allow" "Action": "Service:*"`

Beispielsweise führt die folgende Aussage in einer Richtlinie zu einem fehlgeschlagenen Ergebnis.

```
"Statement": [  
  {  
    "Sid": "EC2-Wildcard",  
    "Effect": "Allow",  
    "Action": "ec2:*",  
    "Resource": "*"   
  }  
]
```

Das Steuerelement schlägt auch fehl, wenn Sie `"Effect": "Allow"` mit `"NotAction": "service:*"` verwenden. In diesem Fall bietet das NotAction Element Zugriff auf alle Aktionen in einem AWS-Service, mit Ausnahme der in angegebenen AktionenNotAction.

Diese Kontrolle gilt nur für vom Kunden verwaltete IAM-Richtlinien. Sie gilt nicht für IAM-Richtlinien, die von verwaltet werden. AWS

Wenn Sie Berechtigungen zuweisen AWS-Services, ist es wichtig, dass Sie den Umfang der zulässigen IAM-Aktionen in Ihren IAM-Richtlinien angeben. Sie sollten IAM-Aktionen nur auf die Aktionen beschränken, die benötigt werden. Auf diese Weise können Sie Berechtigungen mit den geringsten Rechten bereitstellen. Zu freizügige Richtlinien können zu einer Eskalation von Rechten führen, wenn die Richtlinien einem IAM-Prinzipal zugeordnet sind, für den die Genehmigung möglicherweise nicht erforderlich ist.

In einigen Fällen möchten Sie möglicherweise IAM-Aktionen zulassen, die ein ähnliches Präfix haben, z. B. und. `DescribeFlowLogs` `DescribeAvailabilityZones` In diesen autorisierten Fällen können Sie dem allgemeinen Präfix einen Platzhalter mit einem Suffix hinzufügen. Beispiel, `ec2:Describe*`.

Dieses Steuerelement ist erfolgreich, wenn Sie eine IAM-Aktion mit einem Präfix und einem Platzhalter mit Suffix verwenden. Beispielsweise führt die folgende Anweisung in einer Richtlinie zu einem erfolgreichen Ergebnis.

```
"Statement": [  
  {  
    "Sid": "EC2-Wildcard",  
    "Effect": "Allow",  
    "Action": "ec2:Describe*",  
    "Resource": "*"   
  }  
]
```

Wenn Sie verwandte IAM-Aktionen auf diese Weise gruppieren, können Sie auch verhindern, dass die Größenbeschränkungen der IAM-Richtlinie überschritten werden.

Note

AWS Config sollte in allen Regionen aktiviert sein, in denen Sie Security Hub verwenden. Die globale Ressourcenaufzeichnung kann jedoch in einer einzigen Region aktiviert werden. Wenn Sie nur globale Ressourcen in einer einzelnen Region erfassen, können Sie diese Kontrolle in allen Regionen mit Ausnahme der Region deaktivieren, in der Sie globale Ressourcen aufzeichnen.

Abhilfe

Um dieses Problem zu beheben, aktualisieren Sie Ihre IAM-Richtlinien, sodass sie keine vollen „*-Administratorrechte zulassen. Einzelheiten zur Bearbeitung einer IAM-Richtlinie finden Sie unter [Bearbeiten von IAM-Richtlinien im IAM-Benutzerhandbuch](#).

[IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/1.12, CIS Foundations Benchmark v1.4.0/1.12, NIST.800-171.R2 3.1.2 AWS

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: AWS::IAM::User

AWS Config Regel: [iam-user-unused-credentials-check](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob Ihre IAM-Benutzer über Passwörter oder aktive Zugriffsschlüssel verfügen, die 45 Tage oder länger nicht verwendet wurden. Zu diesem Zweck wird geprüft, ob der `maxCredentialUsageAge` Parameter der AWS Config Regel 45 oder mehr beträgt.

Benutzer können mit verschiedenen Arten von Anmeldeinformationen wie Kennwörtern oder Zugriffsschlüsseln auf AWS Ressourcen zugreifen.

CIS empfiehlt, alle Anmeldeinformationen zu entfernen oder zu deaktivieren, die 45 Tage oder länger nicht verwendet wurden. Durch das Deaktivieren oder Entfernen unnötiger Anmeldeinformationen reduzieren Sie den möglichen Schaden, der mit den Anmeldeinformationen eines kompromittierten oder ungenutzten Kontos angerichtet werden kann.

Die AWS Config Regel für dieses Steuerelement verwendet die Operationen [GetCredentialReport](#) und [GenerateCredentialReport](#) API, die nur alle vier Stunden aktualisiert werden. Es kann bis zu vier Stunden dauern, bis Änderungen an IAM-Benutzern für dieses Steuerelement sichtbar sind.

Note

AWS Config sollte in allen Regionen aktiviert sein, in denen Sie Security Hub verwenden. Sie können jedoch die Aufzeichnung globaler Ressourcen in einer einzigen Region aktivieren. Wenn Sie nur globale Ressourcen in einer einzelnen Region erfassen, können Sie diese Kontrolle in allen Regionen mit Ausnahme der Region deaktivieren, in der Sie globale Ressourcen aufzeichnen.

Abhilfe

Wenn Sie Benutzerinformationen in der IAM-Konsole anzeigen, gibt es Spalten für das Alter des Zugriffsschlüssels, das Alter des Kennworts und die letzte Aktivität. Wenn der Wert in einer dieser Spalten mehr als 45 Tage beträgt, deaktivieren Sie die Anmeldeinformationen für diese Benutzer.

Sie können auch [Berichte über Anmeldeinformationen](#) verwenden, um Benutzer zu überwachen und Benutzer zu identifizieren, die 45 oder mehr Tage lang keine Aktivität hatten. Sie können Berichte über Anmeldeinformationen im `.csv` Format von der IAM-Konsole herunterladen.

Nachdem Sie die inaktiven Konten oder ungenutzten Anmeldeinformationen identifiziert haben, deaktivieren Sie sie. Anweisungen finden Sie im IAM-Benutzerhandbuch unter [Erstellen, Ändern oder Löschen eines IAM-Benutzerkennworts \(Konsole\)](#).

[IAM.23] IAM Access Analyzer-Analyzer sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::AccessAnalyzer::Analyzer`

AWS Config Regel: `tagged-accessanalyzer-analyzer` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob ein von AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) verwalteter Analyzer über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter definiert sind. `requiredTagKeys` Das Steuerelement schlägt fehl, wenn der Analyzer keine Tagschlüssel hat oder wenn er nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Analyzer mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Analyzer finden Sie [TagResource](#) in der AWS IAM Access Analyzer API-Referenz.

[IAM.24] IAM-Rollen sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::IAM::Role

AWS Config Regel: tagged-iam-role (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob eine AWS Identity and Access Management (IAM-) Rolle Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind. `requiredTagKeys` Das Steuerelement schlägt fehl, wenn die Rolle keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Rolle mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` , werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer IAM-Rolle finden Sie unter [Tagging IAM-Ressourcen im IAM-Benutzerhandbuch](#).

[IAM.25] IAM-Benutzer sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::IAM::User

AWS Config Regel: tagged-iam-user (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
requiredTagKeys	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob ein AWS Identity and Access Management (IAM-) Benutzer über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter definiert sind. `requiredTagKeys` Das Steuerelement schlägt fehl, wenn der Benutzer keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Benutzer mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem IAM-Benutzer finden Sie unter [Tagging IAM-Ressourcen im IAM-Benutzerhandbuch](#).

[IAM.26] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden

Verwandte Anforderungen: CIS Foundations Benchmark v3.0.0/1.19 AWS

Kategorie: Identifizieren > Konformität

Schweregrad: Mittel

Art der Ressource: AWS::IAM::ServerCertificate

AWS Config Regel: [iam-server-certificate-expiration-check](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Mit dieser Steuerung wird geprüft, ob ein aktives SSL/TLS Serverzertifikat, das in IAM verwaltet wird, abgelaufen ist. Die Kontrolle schlägt fehl, wenn das abgelaufene SSL/TLS Serverzertifikat nicht entfernt wird.

Um HTTPS-Verbindungen zu Ihrer Website oder Anwendung in zu aktivieren AWS, benötigen Sie ein SSL/TLS Serverzertifikat. Sie können IAM oder AWS Certificate Manager (ACM) verwenden, um Serverzertifikate zu speichern und bereitzustellen. Verwenden Sie IAM nur dann als Zertifikatsmanager, wenn Sie HTTPS-Verbindungen in einer Umgebung unterstützen müssen AWS-Region , die von ACM nicht unterstützt wird. IAM bietet eine sichere Verschlüsselungsmethode für Ihre privaten Schlüssel und speichert die verschlüsselte Version in einem SSL-Zertifikatspeicher in IAM. IAM unterstützt die Bereitstellung von Serverzertifikaten in allen Regionen, Sie müssen Ihr Zertifikat jedoch von einem externen Anbieter beziehen, damit Sie es verwenden können. AWS Sie können kein ACM-Zertifikat auf IAM hochladen. Darüber hinaus können Sie Ihre Zertifikate nicht von der IAM-Konsole aus verwalten. Durch das Entfernen abgelaufener SSL/TLS Zertifikate wird das Risiko vermieden, dass versehentlich ein ungültiges Zertifikat für eine Ressource bereitgestellt wird, wodurch die Glaubwürdigkeit der zugrunde liegenden Anwendung oder Website beeinträchtigt werden kann.

Abhilfe

Informationen zum Entfernen eines Serverzertifikats aus IAM finden Sie unter [Verwalten von Serverzertifikaten in IAM](#) im IAM-Benutzerhandbuch.

[IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess

Verwandte Anforderungen: CIS Foundations Benchmark v3.0.0/1.22 AWS

Kategorie: Schützen > Sichere Zugriffsverwaltung > Sichere IAM-Richtlinien

Schweregrad: Mittel

Ressourcentyp: AWS::IAM::Role, AWS::IAM::User AWS::IAM::Group

AWS Config Regel: [iam-policy-blacklisted-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- „policyArns“: „arn:aws:iam::aws:policy/AWSCloudShellFullAccess,arn:aws-cn:iam::aws:policy/AWSCloudShellFullAccess, arn:aws-us-gov:iam::aws:policy/AWSCloudShellFullAccess

Dieses Steuerelement prüft, ob eine IAM-Identität (Benutzer, Rolle oder Gruppe) mit der verwalteten Richtlinie verknüpft ist. AWS AWSCloudShellFullAccess Die Steuerung schlägt fehl, wenn die AWSCloudShellFullAccess Richtlinie an eine IAM-Identität angehängt ist.

AWS CloudShell bietet eine bequeme Möglichkeit, CLI-Befehle auszuführen AWS-Services. Die AWS verwaltete Richtlinie AWSCloudShellFullAccess bietet vollen Zugriff CloudShell auf und ermöglicht somit das Hoch- und Herunterladen von Dateien zwischen dem lokalen System eines Benutzers und der CloudShell Umgebung. Innerhalb der CloudShell Umgebung verfügt ein Benutzer über Sudo-Berechtigungen und kann auf das Internet zugreifen. Das Anhängen dieser verwalteten Richtlinie an eine IAM-Identität gibt ihnen somit die Möglichkeit, Dateiübertragungssoftware zu installieren und Daten von externen Internetservern CloudShell zu verschieben. Wir empfehlen, dem Prinzip der geringsten Rechte zu folgen und Ihren IAM-Identitäten engere Berechtigungen zuzuweisen.

Abhilfe

Informationen zum Trennen der *AWSCloudShellFullAccess* Richtlinie von einer IAM-Identität finden Sie unter [Hinzufügen und Entfernen von IAM-Identitätsberechtigungen im IAM-Benutzerhandbuch](#).

[IAM.28] Der externe Zugriffsanalysator für IAM Access Analyzer sollte aktiviert sein

Verwandte Anforderungen: CIS Foundations Benchmark v3.0.0/1.20 AWS

Kategorie: Erkennen > Erkennungsdienste > Überwachung privilegierter Nutzung

Schweregrad: Hoch

Art der Ressource: AWS::AccessAnalyzer::Analyzer

AWS Config Regel: [iam-external-access-analyzer-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob AWS-Konto ein externer Zugriffsanalysator für IAM Access Analyzer aktiviert ist. Die Steuerung schlägt fehl, wenn für das Konto in Ihrem aktuell ausgewählten AWS-Region Konto kein External Access Analyzer aktiviert ist.

Die externen Zugriffsanalysatoren von IAM Access Analyzer helfen dabei, Ressourcen wie Amazon Simple Storage Service (Amazon S3) -Buckets oder IAM-Rollen zu identifizieren, die mit einer externen Entität gemeinsam genutzt werden. Auf diese Weise können Sie einen unbeabsichtigten Zugriff auf Ihre Ressourcen und Daten vermeiden. IAM Access Analyzer ist regional und muss in jeder Region aktiviert sein. Um Ressourcen zu identifizieren, die gemeinsam mit externen Principals genutzt werden, analysiert ein Access Analyzer die ressourcenbasierten Richtlinien in Ihrer Umgebung anhand von logischen Argumenten. AWS Wenn Sie einen externen Zugriffsanalysator erstellen, können Sie ihn für Ihre gesamte Organisation oder einzelne Konten erstellen und aktivieren.

Note

Wenn ein Konto Teil einer Organisation in ist AWS Organizations, werden externe Zugriffsanalysatoren, die die Organisation als Vertrauenszone angeben und für die Organisation in der aktuellen Region aktiviert sind, bei dieser Steuerung nicht berücksichtigt. Wenn Ihre Organisation diese Art von Konfiguration verwendet, sollten Sie erwägen, diese Steuerung für einzelne Mitgliedskonten in Ihrer Organisation in der Region zu deaktivieren.

Abhilfe

Informationen zur Aktivierung eines externen Access Analyzers in einer bestimmten Region finden Sie unter [Erste Schritte mit IAM Access Analyzer](#) im IAM-Benutzerhandbuch. Sie müssen in jeder Region, in der Sie den Zugriff auf Ihre Ressourcen überwachen möchten, einen Analyzer aktivieren.

Security Hub-Steuerelemente für Amazon Inspector

Diese AWS Security Hub Kontrollen bewerten den Service und die Ressourcen von Amazon Inspector.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[Inspector.1] Das EC2 Scannen mit Amazon Inspector sollte aktiviert sein

Verwandte Anforderungen: PCI DSS v4.0.1/11.3.1

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Hoch

Art der Ressource: AWS:::Account

AWS Config -Regel: [inspector-ec2-scan-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob das EC2 Scannen mit Amazon Inspector aktiviert ist. Bei einem eigenständigen Konto schlägt die Kontrolle fehl, wenn das Amazon EC2 Inspector-Scannen im Konto deaktiviert ist. In einer Umgebung mit mehreren Konten schlägt die Kontrolle fehl, wenn für das delegierte Amazon Inspector-Administratorkonto und alle Mitgliedskonten das EC2 Scannen nicht aktiviert ist.

In einer Umgebung mit mehreren Konten generiert die Kontrolle Ergebnisse nur im delegierten Amazon Inspector-Administratorkonto. Nur der delegierte Administrator kann die EC2 Scanfunktion für die Mitgliedskonten in der Organisation aktivieren oder deaktivieren. Amazon Inspector Inspector-Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Diese Kontrolle generiert FAILED Ergebnisse, wenn der delegierte Administrator über ein gesperrtes Mitgliedskonto verfügt, für das der Amazon EC2 Inspector-Scan nicht aktiviert ist. Um ein PASSED Ergebnis zu erhalten, muss der delegierte Administrator die Zuordnung dieser gesperrten Konten in Amazon Inspector aufheben.

EC2 Das Scannen mit Amazon Inspector extrahiert Metadaten aus Ihrer Amazon Elastic Compute Cloud (Amazon EC2) -Instance und vergleicht diese Metadaten dann mit Regeln, die in Sicherheitsempfehlungen gesammelt wurden, um Ergebnisse zu erzielen. Amazon Inspector scannt Instances auf Paketschwachstellen und Probleme mit der Netzwerkerreichbarkeit. Informationen zu unterstützten Betriebssystemen, einschließlich der Betriebssysteme, die ohne SSM-Agent gescannt werden können, finden Sie unter [Unterstützte Betriebssysteme: EC2 Amazon-Scannen](#).

Abhilfe

Informationen zum Aktivieren von Amazon EC2 Inspector-Scans finden Sie unter [Aktivieren von Scans](#) im Amazon Inspector Inspector-Benutzerhandbuch.

[Inspector.2] Das Amazon Inspector ECR-Scannen sollte aktiviert sein

Verwandte Anforderungen: PCI DSS v4.0.1/11.3.1

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Hoch

Art der Ressource: AWS:::Account

AWS Config -Regel: [inspector-ecr-scan-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob das Amazon Inspector ECR-Scannen aktiviert ist. Bei einem eigenständigen Konto schlägt die Kontrolle fehl, wenn das Amazon Inspector ECR-Scannen im Konto deaktiviert ist. In einer Umgebung mit mehreren Konten schlägt die Kontrolle fehl, wenn für das delegierte Amazon Inspector-Administratorkonto und alle Mitgliedskonten kein ECR-Scan aktiviert ist.

In einer Umgebung mit mehreren Konten generiert die Kontrolle Ergebnisse nur im delegierten Amazon Inspector-Administratorkonto. Nur der delegierte Administrator kann die ECR-Scanfunktion für die Mitgliedskonten in der Organisation aktivieren oder deaktivieren. Amazon Inspector Inspector-Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Diese Kontrolle generiert FAILED Ergebnisse, wenn der delegierte Administrator über ein gesperrtes Mitgliedskonto verfügt, für das der Amazon Inspector ECR-Scan nicht aktiviert ist. Um ein PASSED Ergebnis zu erhalten, muss der delegierte Administrator die Zuordnung dieser gesperrten Konten in Amazon Inspector aufheben.

Amazon Inspector scannt Container-Images, die in Amazon Elastic Container Registry (Amazon ECR) gespeichert sind, auf Softwareschwachstellen, um Sicherheitslücken in Paketen zu ermitteln. Wenn Sie Amazon Inspector-Scans für Amazon ECR aktivieren, legen Sie Amazon Inspector als Ihren bevorzugten Scan-Service für Ihre private Registrierung fest. Dadurch wird das einfache Scannen, das von Amazon ECR kostenlos bereitgestellt wird, durch das erweiterte Scannen

ersetzt, das über Amazon Inspector bereitgestellt und in Rechnung gestellt wird. Das erweiterte Scannen bietet Ihnen den Vorteil des Schwachstellenscans sowohl für Betriebssysteme als auch für Programmiersprachenpakete auf Registrierungsebene. Sie können die Ergebnisse, die mit dem erweiterten Scannen auf Bildebene entdeckt wurden, für jede Ebene des Bilds in der Amazon ECR-Konsole überprüfen. Darüber hinaus können Sie diese Ergebnisse in anderen Diensten überprüfen und mit ihnen arbeiten, die für grundlegende Scanergebnisse nicht verfügbar sind, einschließlich AWS Security Hub Amazon EventBridge.

Abhilfe

Informationen zum Aktivieren von Amazon Inspector ECR-Scans finden Sie unter [Aktivieren von Scans](#) im Amazon Inspector Inspector-Benutzerhandbuch.

[Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein

Verwandte Anforderungen: PCI DSS v4.0.1/6.2.4, PCI DSS v4.0.1/6.3.1

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Hoch

Art der Ressource: AWS:::Account

AWS Config -Regel: [inspector-lambda-code-scan-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob das Scannen von Amazon Inspector Lambda-Code aktiviert ist. Bei einem eigenständigen Konto schlägt die Kontrolle fehl, wenn das Scannen von Amazon Inspector Lambda-Code im Konto deaktiviert ist. In einer Umgebung mit mehreren Konten schlägt die Kontrolle fehl, wenn für das delegierte Amazon Inspector-Administratorkonto und für alle Mitgliedskonten der Lambda-Code-Scan nicht aktiviert ist.

In einer Umgebung mit mehreren Konten generiert die Kontrolle Ergebnisse nur im delegierten Amazon Inspector-Administratorkonto. Nur der delegierte Administrator kann die Lambda-Code-Scanfunktion für die Mitgliedskonten in der Organisation aktivieren oder deaktivieren. Amazon Inspector Inspector-Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Diese Kontrolle generiert FAILED Ergebnisse, wenn der delegierte Administrator ein gesperrtes

Mitgliedskonto hat, für das Amazon Inspector Lambda-Code-Scan nicht aktiviert ist. Um ein PASSED Ergebnis zu erhalten, muss der delegierte Administrator die Zuordnung dieser gesperrten Konten in Amazon Inspector aufheben.

Das Amazon Inspector Lambda-Codescanning scannt den benutzerdefinierten Anwendungscode innerhalb einer AWS Lambda Funktion auf Code-Schwachstellen auf der Grundlage bewährter AWS Sicherheitsmethoden. Durch das Scannen von Lambda-Code können Injektionsfehler, Datenlecks, schwache Kryptografie oder fehlende Verschlüsselung in Ihrem Code erkannt werden. Diese Funktion ist nur in [bestimmten AWS-Regionen](#) Fällen verfügbar. Sie können das Lambda-Code-Scannen zusammen mit dem Lambda-Standardscannen aktivieren (siehe [\[Inspector.4\] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein](#)).

Abhilfe

Informationen zur Aktivierung des Amazon Inspector Lambda-Code-Scans finden Sie unter [Aktivieren von Scans](#) im Amazon Inspector Inspector-Benutzerhandbuch.

[Inspector.4] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein

Verwandte Anforderungen: PCI DSS v4.0.1/6.2.4, PCI DSS v4.0.1/6.3.1

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Hoch

Art der Ressource: AWS:::Account

AWS Config -Regel: [inspector-lambda-standard-scan-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob das Standardscannen von Amazon Inspector Lambda aktiviert ist. Bei einem eigenständigen Konto schlägt die Kontrolle fehl, wenn der Amazon Inspector Lambda-Standardscan im Konto deaktiviert ist. In einer Umgebung mit mehreren Konten schlägt die Kontrolle fehl, wenn für das delegierte Amazon Inspector-Administratorkonto und alle Mitgliedskonten das Lambda-Standardscannen nicht aktiviert ist.

In einer Umgebung mit mehreren Konten generiert die Kontrolle Ergebnisse nur im delegierten Amazon Inspector-Administratorkonto. Nur der delegierte Administrator kann die Lambda-

Standardscanfunktion für die Mitgliedskonten in der Organisation aktivieren oder deaktivieren. Amazon Inspector Inspector-Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Diese Kontrolle generiert FAILED Ergebnisse, wenn der delegierte Administrator ein gesperrtes Mitgliedskonto hat, für das Amazon Inspector Lambda Standard-Scan nicht aktiviert ist. Um ein PASSED Ergebnis zu erhalten, muss der delegierte Administrator die Zuordnung dieser gesperrten Konten in Amazon Inspector aufheben.

Das Standard-Scannen von Amazon Inspector Lambda identifiziert Softwareschwachstellen in den Abhängigkeiten von Anwendungspaketen, die Sie Ihrem AWS Lambda Funktionscode und Ihren Ebenen hinzufügen. Wenn Amazon Inspector eine Sicherheitslücke in den Abhängigkeiten Ihrer Lambda-Funktionsanwendung feststellt, erstellt Amazon Inspector eine detaillierte Package Vulnerability Typfindung. Sie können das Lambda-Code-Scannen zusammen mit dem Lambda-Standardscannen aktivieren (siehe [\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)).

Abhilfe

Informationen zur Aktivierung von Amazon Inspector Lambda-Standardscans finden Sie unter [Aktivieren von Scans](#) im Amazon Inspector Inspector-Benutzerhandbuch.

Security Hub-Steuerungen für AWS IoT

Diese AWS Security Hub Kontrollen bewerten den AWS IoT Service und die Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[IoT.1] AWS IoT Device Defender Sicherheitsprofile sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::IoT::SecurityProfile

AWS Config Regel: tagged-iot-securityprofile (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob ein AWS IoT Device Defender Sicherheitsprofil Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn das Sicherheitsprofil keine Tagschlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel enthält `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Sicherheitsprofil mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS IoT Device Defender Sicherheitsprofil finden Sie unter [Taggen Ihrer AWS IoT Ressourcen im AWS IoT Entwicklerhandbuch](#).

[IoT.2] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoT::MitigationAction`

AWS Config Regel: `tagged-iot-mitigationaction` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob eine AWS IoT Core Schadensbegrenzungsaktion über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter definiert sind. `requiredTagKeys` Die Steuerung schlägt fehl, wenn die Abhilfemaßnahme keine Tagschlüssel hat oder wenn nicht alle im Parameter angegebenen Schlüssel vorhanden sind. `requiredTagKeys` Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Abhilfemaßnahme mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS IoT Core Schadensbegrenzungsmaßnahme finden Sie unter [Taggen Ihrer AWS IoT Ressourcen](#) im Entwicklerhandbuch.AWS IoT

[IoT.3] AWS IoT Core -Dimensionen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoT::Dimension`

AWS Config Regel: `tagged-iot-dimension` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob eine AWS IoT Core Dimension über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn die Dimension keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Dimension mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginaws :` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien

für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS IoT Core Dimension finden Sie unter [Taggen Ihrer AWS IoT Ressourcen im AWS IoT Entwicklerhandbuch](#).

[IoT.4] AWS IoT Core Autorisierer sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoT::Authorizer`

AWS Config Regel: `tagged-iot-authorizer` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS	No default value

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen.	

Dieses Steuerelement prüft, ob ein AWS IoT Core Autorisierer über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter definiert sind. `requiredTagKeys` Das Steuerelement schlägt fehl, wenn der Autorisierer keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat. `requiredTagKeys` Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Autorisierer mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` , werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS IoT Core Autorisierer finden Sie unter [Taggen Ihrer AWS IoT Ressourcen](#) im Entwicklerhandbuch.AWS IoT

[IoT.5] AWS IoT Core Rollenalias sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoT::RoleAlias`

AWS Config Regel: `tagged-iot-rolealias` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob ein AWS IoT Core Rollenalias Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn der Rollenalias keine Tagschlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Rollenalias mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS IoT Core Rollenalias finden Sie unter [Taggen Ihrer AWS IoT Ressourcen im AWS IoT Entwicklerhandbuch](#).

[IoT.6] AWS IoT Core Richtlinien sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoT::Policy`

AWS Config Regel: `tagged-iot-policy` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob eine AWS IoT Core Richtlinie Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn die Richtlinie keine Tagschlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Richtlinie mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `aws:*` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS IoT Core Richtlinie finden Sie unter [Taggen Ihrer AWS IoT Ressourcen im AWS IoT Entwicklerhandbuch](#).

Security Hub-Steuerungen für AWS IoT Events

Diese AWS Security Hub Kontrollen bewerten den Dienst und die Ressourcen von AWS IoT Events.

Diese Steuerungen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[IoTEvents .1] AWS IoT-Events-Eingaben sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoTEvents::Input`

AWS Config -Regel: `iotevents-input-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS IoT-Events-Eingabe Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind `requiredKeyTags`. Das Steuerelement schlägt fehl, wenn die Eingabe keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält `requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Eingabe mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `aws:*` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS IoT-Ereigniseingabe finden Sie unter [Taggen Ihrer AWS IoT Events Ressourcen](#) im AWS IoT Events Entwicklerhandbuch.

[IoT Events .2] AWS IoT-Ereignisdetektormodelle sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoTEvents::DetectorModel`

AWS Config -Regel: `iotevents-detector-model-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS IoT-Ereignisdetektormodell Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind `requiredKeyTags`. Die Steuerung schlägt fehl, wenn das Detektormodell keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel hat `requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft die Steuerung nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Detektormodell mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` , werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS IoT-Ereignisdetektormodell finden Sie unter [Taggen Ihrer AWS IoT Events Ressourcen](#) im AWS IoT Events Entwicklerhandbuch.

[IoT Events .3] Alarmmodelle für AWS IoT Events sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoTEvents::AlarmModel`

AWS Config -Regel: `iotevents-alarm-model-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Diese Steuerung prüft, ob ein AWS IoT-Events-Alarmmodell Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind `requiredKeyTags`. Die Steuerung schlägt fehl, wenn das Alarmmodell keine Tag-Schlüssel hat oder wenn nicht alle im Parameter angegebenen Schlüssel vorhanden sind `requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft die Steuerung nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Alarmmodell mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `aws:*` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen

anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS IoT-Ereignis-Alarmmodell finden Sie unter [Taggen Ihrer AWS IoT Events Ressourcen](#) im AWS IoT Events Entwicklerhandbuch.

Security Hub-Steuerungen für AWS IoT SiteWise

Diese AWS Security Hub Kontrollen bewerten den AWS SiteWise IoT-Dienst und die Ressourcen.

Diese Steuerungen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[IoT Site Wise.1] AWS SiteWise IoT-Asset-Modelle sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoTSiteWise::AssetModel`

AWS Config -Regel: `iotsitewise-asset-model-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS SiteWise IoT-Asset-Modell Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind `requiredKeyTags`. Das Steuerelement schlägt fehl, wenn das Asset-Modell keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel hat `requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Asset-Modell mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS SiteWise IoT-Assetmodell finden Sie unter [Taggen Ihrer AWS IoT SiteWise Ressourcen](#) im AWS IoT SiteWise Benutzerhandbuch.

[IoT SiteWise.2] AWS SiteWise IoT-Dashboards sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoTSiteWise::Dashboard`

AWS Config -Regel: `iotsitewise-dashboard-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS SiteWise IoT-Dashboard Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind `requiredKeyTags`. Das Steuerelement schlägt fehl, wenn das Dashboard keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel enthält `requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Dashboard mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` , werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS SiteWise IoT-Dashboard finden Sie unter [Taggen Ihrer AWS IoT SiteWise Ressourcen](#) im AWS IoT SiteWise Benutzerhandbuch.

[IoT Site Wise.3] AWS SiteWise IoT-Gateways sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoTSiteWise::Gateway`

AWS Config -Regel: `iotsitewise-gateway-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS SiteWise IoT-Gateway über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter definiert sind `requiredKeyTags`. Die Steuerung schlägt fehl, wenn das Gateway keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel hat `requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Gateway mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen

anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS SiteWise IoT-Gateway finden Sie unter [Taggen Ihrer AWS IoT SiteWise Ressourcen](#) im AWS IoT SiteWise Benutzerhandbuch.

[Io TSite Wise.4] AWS SiteWise IoT-Portale sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoTSiteWise::Portal`

AWS Config -Regel: `iotsitewise-portal-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS	Kein Standardwert

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen.	

Dieses Steuerelement prüft, ob ein AWS SiteWise IoT-Portal Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind `requiredKeyTags`. Das Steuerelement schlägt fehl, wenn das Portal keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel hat `requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Portal mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `aws:` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter

AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS SiteWise IoT-Portal finden Sie unter [Taggen Ihrer AWS IoT SiteWise Ressourcen](#) im AWS IoT SiteWise Benutzerhandbuch.

[IoT SiteWise.5] AWS SiteWise IoT-Projekte sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::IoTSiteWise::Project

AWS Config -Regel: iotsitewise-project-tagged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
requiredKeyTags	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS SiteWise IoT-Projekt Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind `requiredKeyTags`. Das Steuerelement schlägt fehl, wenn das Projekt keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel

`requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Projekt mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS SiteWise IoT-Projekt finden Sie unter [Taggen Ihrer AWS IoT SiteWise Ressourcen](#) im AWS IoT SiteWise Benutzerhandbuch.

Security Hub-Steuerungen für das AWS IoT TwinMaker

Diese AWS Security Hub Kontrollen bewerten den AWS TwinMaker IoT-Dienst und die Ressourcen.

Diese Steuerungen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[IoT Twin Maker.1] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoT::TwinMaker::SyncJob`

AWS Config -Regel: `iottwinmaker-sync-job-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS TwinMaker IoT-Synchronisierungsjob Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind `requiredKeyTags`. Die Steuerung schlägt fehl, wenn der Synchronisierungsauftrag keine Tag-Schlüssel hat oder wenn nicht alle im Parameter angegebenen Schlüssel vorhanden sind `requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Synchronisierungsauftrag mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginaws:` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck,

Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS TwinMaker IoT-Synchronisierungsjob finden Sie unter [TagResource](#) im AWS IoT TwinMaker -Benutzerhandbuch.

[IoT Twin Maker.2] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoT::TwinMaker::Workspace`

AWS Config -Regel: `iottwinmaker-workspace-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS TwinMaker IoT-Workspace Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind `requiredKeyTags`. Das Steuerelement schlägt fehl, wenn der Workspace keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat `requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Workspace mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

 **Note**

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS TwinMaker IoT-Workspace finden Sie unter [TagResource](#) im AWS IoT TwinMaker -Benutzerhandbuch.

[IoT Twin Maker.3] AWS TwinMaker IoT-Szenen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoT::TwinMaker::Scene`

AWS Config -Regel: `iottwinmaker-scene-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS TwinMaker IoT-Szene Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind `requiredKeyTags`. Die Steuerung schlägt fehl, wenn die Szene keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat `requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Szene mit keinem Schlüssel markiert ist. System-Tags, die automatisch angewendet werden und mit `beginnenaws :` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS TwinMaker IoT-Szene finden Sie unter [TagResource](#) im AWS IoT TwinMaker -Benutzerhandbuch.

[IoT Twin Maker.4] AWS TwinMaker IoT-Entitäten sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoT::TwinMaker::Entity`

AWS Config -Regel: `iottwinmaker-entity-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS TwinMaker IoT-Entität Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind `requiredKeyTags`. Das Steuerelement schlägt fehl, wenn die Entität keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat `requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Entität mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `aws:*` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen

anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS TwinMaker IoT-Entität finden Sie unter [TagResource](#) im AWS IoT TwinMaker -Benutzerhandbuch.

Security Hub-Steuerungen für AWS IoT Wireless

Diese AWS Security Hub Kontrollen bewerten den AWS IoT-Wireless-Service und die Ressourcen.

Diese Steuerungen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[IoTWireless .1] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoTWireless::MulticastGroup`

AWS Config -Regel: `iotwireless-multicast-group-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS IoT Wireless Wireless-Multicast-Gruppe Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredKeyTags` definiert sind. Die Steuerung schlägt fehl, wenn die Multicast-Gruppe keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat. `requiredKeyTags` Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Multicast-Gruppe mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS IoT-Wireless-Multicast-Gruppe finden Sie unter [Taggen Ihrer AWS IoT Wireless Ressourcen](#) im AWS IoT Wireless Entwicklerhandbuch.

[Io TWireless .2] AWS IoT-Wireless-Dienstprofile sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoTWireless::ServiceProfile`

AWS Config -Regel: `iotwireless-service-profile-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS IoT Wireless Wireless-Dienstprofil Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind `requiredKeyTags`. Die Steuerung schlägt fehl, wenn das Dienstprofil keine Tagschlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel enthält `requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Dienstprofil mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS IoT Wireless Wireless-Dienstprofil finden Sie unter [Taggen Ihrer AWS IoT Wireless Ressourcen](#) im AWS IoT Wireless Entwicklerhandbuch.

[IoT Wireless .3] AWS IoT FUOTA-Aufgaben sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoTWireless::FuotaTask`

AWS Config -Regel: `iotwireless-fuota-task-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS IoT Wireless Firmware Update over-the-air (FUOTA) -Task Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredKeyTags` definiert sind. Die Steuerung schlägt fehl, wenn die FUOTA-Aufgabe keine Tag-Schlüssel hat oder wenn nicht alle im Parameter angegebenen Schlüssel vorhanden sind. `requiredKeyTags` Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die FUOTA-Aufgabe mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws:` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen

anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS IoT Wireless FUOTA-Aufgabe finden Sie unter [Tagging your AWS IoT Wireless resources](#) im AWS IoT Wireless Developer Guide.

Security Hub-Steuerelemente für Amazon IVS

Diese AWS Security Hub Kontrollen bewerten den Service und die Ressourcen des Amazon Interactive Video Service (IVS).

Diese Steuerungen sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[IVS.1] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IVS::PlaybackKeyPair`

AWS Config -Regel: `ivs-playback-key-pair-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon IVS-Wiedergabeschlüsselpaar Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredKeyTags` definiert sind. Die Steuerung schlägt fehl, wenn das Playback-Schlüsselpaar keine Tag-Tasten hat oder wenn es nicht alle im Parameter angegebenen Tasten hat `requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Playback-Schlüsselpaar mit keinem Schlüssel markiert ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem IVS-Wiedergabeschlüsselpaar finden Sie unter [TagResource](#) in der Amazon IVS Real-Time Streaming API-Referenz.

[IVS.2] IVS-Aufzeichnungskonfigurationen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IVS::RecordingConfiguration`

AWS Config -Regel: `ivs-recording configuration-tagged`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon IVS-Aufzeichnungskonfiguration Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredKeyTags` definiert sind. Die Steuerung schlägt fehl, wenn die Aufzeichnungskonfiguration keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter `requiredKeyTags` angegebenen Schlüssel enthält. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Aufzeichnungskonfiguration mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer IVS-Aufzeichnungskonfiguration finden Sie unter [TagResource](#) in der Amazon IVS Real-Time Streaming API-Referenz.

[IVS.3] IVS-Kanäle sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::IVS::Channel

AWS Config -Regel: ivs-channel-tagged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon IVS-Kanal Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredKeyTags` definiert sind. Die Steuerung schlägt fehl, wenn der Kanal keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter `requiredKeyTags` angegebenen Schlüssel hat. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Kanal mit keinem Schlüssel markiert ist. System-Tags, die automatisch angewendet werden und mit `beginnewaws:` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien

für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem IVS-Kanal finden Sie unter [TagResource](#) in der Amazon IVS Real-Time Streaming API-Referenz.

Security Hub-Steuerelemente für Amazon Keyspaces

Diese AWS Security Hub Kontrollen bewerten den Service und die Ressourcen von Amazon Keyspaces.

Diese Kontrollen sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[Keyspaces.1] Amazon Keyspaces Keyspaces sollten mit Tags versehen sein

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::Cassandra::Keyspace

AWS Config -Regel: cassandra-keyspace-tagged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon Keyspaces-Schlüsselraum Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind. `requiredKeyTags` Die Steuerung schlägt fehl, wenn der Schlüsselraum keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält. `requiredKeyTags` Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Schlüsselraum mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Amazon Keyspaces-Schlüsselraum finden [Sie unter Hinzufügen von Tags zu einem Schlüsselraum im Amazon Keyspaces-Entwicklerhandbuch](#).

Security Hub-Steuerelemente für Kinesis

Diese AWS Security Hub Kontrollen bewerten den Service und die Ressourcen von Amazon Kinesis.

Diese Kontrollen sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[Kinesis.1] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 (1), (10), NIST.800-53.R5 NIST.800-53.r5 SC-2 SI-7 NIST.800-53.r5 SC-7 (6)

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: AWS::Kinesis::Stream

AWS Config -Regel: [kinesis-stream-encrypted](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Kinesis Data Streams im Ruhezustand mit serverseitiger Verschlüsselung verschlüsselt sind. Diese Steuerung schlägt fehl, wenn ein Kinesis-Stream im Ruhezustand nicht mit serverseitiger Verschlüsselung verschlüsselt ist.

Serverseitige Verschlüsselung ist eine Funktion in Amazon Kinesis Data Streams, die Daten automatisch verschlüsselt, bevor sie sich im Ruhezustand befinden, mithilfe eines AWS KMS key. Die Daten werden verschlüsselt, bevor sie in die Speicherschicht des Kinesis-Streams geschrieben werden. Nach Abruf aus dem Speicher werden sie entschlüsselt. Daher werden Ihre Daten im Ruhezustand innerhalb des Amazon Kinesis Data Streams Streams-Service verschlüsselt.

Abhilfe

Informationen zur Aktivierung der serverseitigen Verschlüsselung für Kinesis-Streams finden Sie unter [Wie fange ich mit serverseitiger Verschlüsselung an?](#) im Amazon Kinesis Developer Guide.

[Kinesis.2] Kinesis-Streams sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Kinesis::Stream`

AWS Config Regel: `tagged-kinesis-stream` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplanytyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon Kinesis Kinesis-Datenstream Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt

fehl, wenn der Datenstream keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Datenstrom mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` , werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Kinesis-Datenstream finden Sie unter [Tagging your streams in Amazon Kinesis Data Streams](#) im Amazon Kinesis Developer Guide.

[Kinesis.3] Kinesis-Streams sollten über eine angemessene Aufbewahrungsfrist für Daten verfügen

Schweregrad: Mittel

Ressourcentyp: `AWS::Kinesis::Stream`

AWS Config-Regel: [kinesis-stream-backup-retention-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
minimumBackupRetentionPeriod	Mindestanzahl von Stunden, für die die Daten aufbewahrt werden sollen.	String	24 bis 8760	168

Dieses Steuerelement prüft, ob ein Amazon Kinesis Kinesis-Datenstream eine Datenaufbewahrungsdauer hat, die größer oder gleich dem angegebenen Zeitraum ist. Die Kontrolle schlägt fehl, wenn die Datenaufbewahrungsdauer den angegebenen Zeitraum unterschreitet. Sofern Sie keinen benutzerdefinierten Parameterwert für die Datenaufbewahrungsdauer angeben, verwendet Security Hub einen Standardwert von 168 Stunden.

In Kinesis Data Streams ist ein Datenstrom eine geordnete Abfolge von Datensätzen, in die in Echtzeit geschrieben und daraus gelesen werden soll. Datensätze werden vorübergehend in Shards in Ihrem Stream gespeichert. Der Zeitraum ab dem Hinzufügen eines Datensatzes bis zu dem Zeitpunkt, an dem er nicht mehr verfügbar ist, wird als Aufbewahrungszeitraum bezeichnet. Kinesis Data Streams macht Datensätze, die älter als die neue Aufbewahrungsfrist sind, fast sofort unzugänglich, nachdem die Aufbewahrungsfrist verkürzt wurde. Beispielsweise bedeutet eine Änderung des Aufbewahrungszeitraums von 24 Stunden auf 48 Stunden, dass Datensätze, die 23 Stunden und 55 Minuten vorher zum Stream hinzugefügt wurden, nach 24 Stunden weiterhin verfügbar sind.

Abhilfe

Informationen zum Ändern der Aufbewahrungsdauer von Backups für Ihre Kinesis Data Streams finden Sie unter [Ändern der Datenaufbewahrungsdauer](#) im Amazon Kinesis Data Streams Developer Guide.

Security Hub-Steuerungen für AWS KMS

Diese AWS Security Hub Kontrollen bewerten den AWS Key Management Service (AWS KMS) Dienst und die Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen

Verwandte Anforderungen: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6 (3) NIST.800-53.r5 AC-6

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: AWS::IAM::Policy

AWS Config -Regel: [iam-customer-policy-blocked-kms-actions](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `blockedActionsPatterns`: `kms:ReEncryptFrom`, `kms:Decrypt`(nicht anpassbar)
- `excludePermissionBoundaryPolicy`: `True` (nicht anpassbar)

Überprüft, ob die Standardversion der vom Kunden verwalteten IAM-Richtlinien es Prinzipalen erlaubt, die AWS KMS Entschlüsselungsaktionen für alle Ressourcen zu verwenden. Die Steuerung schlägt fehl, wenn die Richtlinie offen genug ist, um `kms:ReEncryptFrom` Aktionen für alle `kms:Decrypt` KMS-Schlüssel zuzulassen.

Das Steuerelement überprüft nur KMS-Schlüssel im Resource-Element und berücksichtigt keine Bedingungen im Condition-Element einer Richtlinie. Darüber hinaus bewertet das Steuerelement sowohl angehängte als auch nicht verknüpfte, vom Kunden verwaltete Richtlinien. Inline-Richtlinien oder AWS verwaltete Richtlinien werden nicht geprüft.

Damit kontrollieren Sie AWS KMS, wer Ihre KMS-Schlüssel verwenden und auf Ihre verschlüsselten Daten zugreifen kann. IAM-Richtlinien definieren, welche Aktionen eine Identität (Benutzer, Gruppe oder Rolle) auf welchen Ressourcen ausführen kann. Gemäß den bewährten Sicherheitsmethoden

wird AWS empfohlen, die geringsten Rechte zuzulassen. Mit anderen Worten, Sie sollten Identitäten nur die `kms:ReEncryptFrom` Berechtigungen `kms:Decrypt` oder und nur die Schlüssel gewähren, die zur Ausführung einer Aufgabe erforderlich sind. Andernfalls verwendet der Benutzer möglicherweise Schlüssel, die für Ihre Daten nicht geeignet sind.

Anstatt Berechtigungen für alle Schlüssel zu gewähren, sollten Sie die Mindestanzahl an Schlüsseln festlegen, die Benutzer für den Zugriff auf verschlüsselte Daten benötigen. Entwerfen Sie dann Richtlinien, die es Benutzern ermöglichen, nur diese Schlüssel zu verwenden. Erlauben Sie beispielsweise nicht die `kms:Decrypt` Erlaubnis für alle KMS-Schlüssel. Erlauben Sie stattdessen `kms:Decrypt` nur Schlüssel in einer bestimmten Region für Ihr Konto. Durch die Anwendung des Prinzips der geringsten Rechte können Sie das Risiko einer unbeabsichtigten Offenlegung Ihrer Daten verringern.

Abhilfe

Informationen zum Ändern einer vom Kunden verwalteten IAM-Richtlinie finden Sie unter [Bearbeiten von kundenverwalteten Richtlinien](#) im IAM-Benutzerhandbuch. Wenn Sie Ihre Richtlinie bearbeiten, geben Sie für das `Resource` Feld den Amazon-Ressourcennamen (ARN) des spezifischen Schlüssels oder der Schlüssel an, für die Sie Entschlüsselungsaktionen zulassen möchten.

[KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen

Verwandte Anforderungen: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7),, NIST.800-53.r5 AC-3 (3) NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6 NIST.800-53.r5 AC-6

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource:

- `AWS::IAM::Group`
- `AWS::IAM::Role`
- `AWS::IAM::User`

AWS Config -Regel: [iam-inline-policy-blocked-kms-actions](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `blockedActionsPatterns`: `kms:ReEncryptFrom`, `kms:Decrypt`(nicht anpassbar)

Dieses Steuerelement prüft, ob die in Ihre IAM-Identitäten (Rolle, Benutzer oder Gruppe) eingebetteten Inline-Richtlinien die AWS KMS Entschlüsselung und erneute Verschlüsselung aller KMS-Schlüssel zulassen. Die Steuerung schlägt fehl, wenn die Richtlinie offen genug ist, um `kms:ReEncryptFrom` Aktionen für alle `kms:Decrypt` KMS-Schlüssel zuzulassen.

Das Steuerelement überprüft nur KMS-Schlüssel im Resource-Element und berücksichtigt keine Bedingungen im Condition-Element einer Richtlinie.

Mit steuern Sie AWS KMS, wer Ihre KMS-Schlüssel verwenden und auf Ihre verschlüsselten Daten zugreifen kann. IAM-Richtlinien definieren, welche Aktionen eine Identität (Benutzer, Gruppe oder Rolle) auf welchen Ressourcen ausführen kann. Gemäß den bewährten Sicherheitsmethoden wird AWS empfohlen, die geringsten Rechte zuzulassen. Mit anderen Worten, Sie sollten Identitäten nur die Berechtigungen gewähren, die sie benötigen, und nur für Schlüssel, die zur Ausführung einer Aufgabe erforderlich sind. Andernfalls verwendet der Benutzer möglicherweise Schlüssel, die für Ihre Daten nicht geeignet sind.

Anstatt die Erlaubnis für alle Schlüssel zu erteilen, sollten Sie die Mindestanzahl an Schlüsseln festlegen, die Benutzer für den Zugriff auf verschlüsselte Daten benötigen. Entwerfen Sie dann Richtlinien, die es den Benutzern ermöglichen, nur diese Schlüssel zu verwenden. Erlauben Sie beispielsweise nicht die `kms:Decrypt` Erlaubnis für alle KMS-Schlüssel. Erlauben Sie die Erlaubnis stattdessen nur für bestimmte Schlüssel in einer bestimmten Region für Ihr Konto. Indem Sie das Prinzip der geringsten Rechte anwenden, können Sie das Risiko einer unbeabsichtigten Offenlegung Ihrer Daten verringern.

Abhilfe

Informationen zum Ändern einer IAM-Inline-Richtlinie finden Sie unter [Bearbeiten von Inline-Richtlinien](#) im IAM-Benutzerhandbuch. Wenn Sie Ihre Richtlinie bearbeiten, geben Sie für das `Resource` Feld den Amazon-Ressourcennamen (ARN) des spezifischen Schlüssels oder der Schlüssel an, für die Sie Entschlüsselungsaktionen zulassen möchten.

[KMS.3] AWS KMS keys sollte nicht unbeabsichtigt gelöscht werden

Verwandte Anforderungen: NIST.800-53.r5 SC-1 2, 2 (NIST.800-53.r5 SC-12)

Kategorie: Schützen > Datenschutz > Schutz vor Datenlöschung

Schweregrad: Kritisch

Art der Ressource: AWS::KMS::Key

AWS Config Regel: kms-cmk-not-scheduled-for-deletion-2 (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Löschung von KMS-Schlüsseln geplant ist. Die Steuerung schlägt fehl, wenn das Löschen eines KMS-Schlüssels geplant ist.

KMS-Schlüssel können nach dem Löschen nicht wiederhergestellt werden. Mit einem KMS-Schlüssel verschlüsselte Daten können auch dauerhaft nicht wiederhergestellt werden, wenn der KMS-Schlüssel gelöscht wird. Wenn aussagekräftige Daten unter einem KMS-Schlüssel verschlüsselt wurden, der gelöscht werden soll, sollten Sie erwägen, die Daten zu entschlüsseln oder die Daten erneut mit einem neuen KMS-Schlüssel zu verschlüsseln, sofern Sie nicht absichtlich eine kryptografische Löschung durchführen.

Wenn das Löschen eines KMS-Schlüssels geplant ist, wird eine obligatorische Wartezeit durchgesetzt, damit genügend Zeit zur Verfügung steht, um den Löschvorgang rückgängig zu machen, falls er versehentlich geplant wurde. Die standardmäßige Wartezeit beträgt 30 Tage, kann aber auf bis zu 7 Tage reduziert werden, wenn der KMS-Schlüssel gelöscht werden soll. Während der Wartezeit kann das geplante Löschen abgebrochen werden und der KMS-Schlüssel wird nicht gelöscht.

Weitere Informationen zum Löschen von KMS-Schlüsseln finden Sie unter [Löschen von KMS-Schlüsseln](#) im AWS Key Management Service Entwicklerhandbuch.

Abhilfe

Informationen zum Abbrechen einer geplanten Löschung von KMS-Schlüsseln finden Sie im AWS Key Management Service Entwicklerhandbuch unter So brechen Sie das Löschen [von Schlüsseln ab \(Konsole\) unter So brechen Sie das Löschen](#) von Schlüsseln ab.

[KMS.4] Die AWS KMS Schlüsselrotation sollte aktiviert sein

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/3.6, CIS Foundations Benchmark v1.4.0/3.8, CIS AWS Foundations Benchmark v1.2.0/2.8, 2 (NIST.800-53.r5 SC-12), 8 (3), PCI DSS v3.2.1/3.6.4, NIST.800-53.r5 SC-1 PCI DSS v4.0.1/3.7.4 AWS NIST.800-53.r5 SC-2

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: AWS::KMS::Key

AWS Config -Regel: [cmk-backing-key-rotation-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

AWS KMS ermöglicht Kunden die Rotation des Backing-Schlüssels, bei dem es sich um Schlüsselmaterial handelt, das im KMS-Schlüssel gespeichert ist AWS KMS und mit der Schlüssel-ID des KMS-Schlüssels verknüpft ist. Der Unterstützungsschlüssel wird zum Durchführen kryptografischer Vorgänge wie z. B. Ver- und Entschlüsselungen verwendet. Die automatische Schlüsselrotation speichert derzeit alle vorherigen Unterstützungsschlüssel, sodass eine transparente Entschlüsselung verschlüsselter Daten erfolgen kann.

CIS empfiehlt, die KMS-Schlüsselrotation zu aktivieren. Das Rotieren der Verschlüsselungsschlüssel trägt zur Verringerung der potenziellen Auswirkungen eines kompromittierten Schlüssels bei, da der Zugriff auf mit einem neuen Schlüssel verschlüsselte Daten mit einem vorherigen Schlüssel, der möglicherweise kompromittiert wurde, nicht möglich ist.

Abhilfe

Informationen zur Aktivierung der KMS-Schlüsselrotation finden Sie unter [So aktivieren und deaktivieren Sie die automatische Schlüsselrotation](#) im AWS Key Management Service Entwicklerhandbuch.

[KMS.5] KMS-Schlüssel sollten nicht öffentlich zugänglich sein

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Kritisch

Art der Ressource: AWS::KMS::Key

AWS Config -Regel: [kms-key-policy-no-public-access](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dadurch wird geprüft, ob ein öffentlich zugänglich AWS KMS key ist. Die Steuerung schlägt fehl, wenn der KMS-Schlüssel öffentlich zugänglich ist.

Die Implementierung des Zugriffs mit den geringsten Rechten ist von grundlegender Bedeutung, um das Sicherheitsrisiko und die Auswirkungen von Fehlern oder böswilligen Absichten zu verringern. Wenn die Schlüsselrichtlinie für ein den Zugriff von externen Konten aus AWS KMS key zulässt, können Dritte möglicherweise Daten mithilfe des Schlüssels ver- und entschlüsseln. Dies könnte dazu führen, dass eine interne oder externe Bedrohung Daten aus dem System herausfiltert, AWS-Services das den Schlüssel verwendet.

 Note

Dieses Steuerelement gibt auch ein FAILED Ergebnis zurück, AWS KMS key wenn Ihre Konfigurationen AWS Config verhindern, dass die Schlüsselrichtlinie im Konfigurationselement (CI) für den KMS-Schlüssel aufgezeichnet wird. Damit die Schlüsselrichtlinie im CI für AWS Config den KMS-Schlüssel aufgefüllt werden kann, muss die [AWS Config Rolle](#) Zugriff haben, um die Schlüsselrichtlinie mithilfe des [GetKeyPolicy](#) API-Aufrufs lesen zu können. Um diese Art von Problem zu beheben FAILED, überprüfen Sie die Richtlinien, die verhindern können, dass die AWS Config Rolle Lesezugriff auf die Schlüsselrichtlinie für den KMS-Schlüssel hat. Überprüfen Sie beispielsweise Folgendes:

- Die Schlüsselrichtlinie für den KMS-Schlüssel.
- Die darin enthaltenen [Dienststeuerungsrichtlinien \(SCPs\)](#) und [Ressourcensteuerungsrichtlinien \(RCPs\)](#) gelten für Ihr Konto. AWS Organizations
- Berechtigungen für die AWS Config Rolle, wenn Sie die [AWS Config dienstverknüpfte Rolle](#) nicht verwenden.

Darüber hinaus bewertet dieses Steuerelement keine Richtlinienbedingungen, die Platzhalterzeichen oder Variablen verwenden. Um ein PASSED Ergebnis zu erzielen, dürfen Bedingungen in der Schlüsselrichtlinie nur feste Werte verwenden, d. h. Werte, die keine Platzhalterzeichen oder Richtlinienvariablen enthalten. Informationen zu Richtlinienvariablen finden Sie unter [Variablen und Tags](#) im AWS Identity and Access Management Benutzerhandbuch.

Abhilfe

Informationen zur Aktualisierung der wichtigsten Richtlinien für eine AWS KMS key finden Sie unter [Wichtige Richtlinien AWS KMS im AWS Key Management Service](#) Entwicklerhandbuch.

Security Hub-Steuerungen für AWS Lambda

Diese AWS Security Hub Kontrollen bewerten den AWS Lambda Service und die Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[Lambda.1] Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten

Verwandte Anforderungen: NIST.800-53.r5 AC-2 1,, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3, (21), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (11), (16) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/7.2.1 PCI DSS v4.0.1/7.2.1 NIST.800-53.r5 SC-7

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Kritisch

Art der Ressource: `AWS::Lambda::Function`

AWS Config -Regel: [lambda-function-public-access-prohibited](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die ressourcenbasierte Richtlinie der Lambda-Funktion den öffentlichen Zugriff außerhalb Ihres Kontos verbietet. Die Kontrolle schlägt fehl, wenn der öffentliche Zugriff zulässig ist. Die Kontrolle schlägt auch fehl, wenn eine Lambda-Funktion von Amazon S3 aus aufgerufen wird und die Richtlinie keine Bedingung zur Beschränkung des öffentlichen Zugriffs enthält, wie z. `AWS:SourceAccount` Wir empfehlen, andere S3-Bedingungen zusammen mit `AWS:SourceAccount` in Ihrer Bucket-Richtlinie zu verwenden, um den Zugriff zu verfeinern.

 Note

Dieses Steuerelement bewertet keine Richtlinienbedingungen, die Platzhalterzeichen oder Variablen verwenden. Um ein PASSED Ergebnis zu erzielen, dürfen Bedingungen in der Richtlinie für die Lambda-Funktion nur feste Werte verwenden, d. h. Werte, die keine Platzhalterzeichen oder Richtlinienvariablen enthalten. Informationen zu Richtlinienvariablen finden Sie unter [Variablen und Tags](#) im AWS Identity and Access Management Benutzerhandbuch.

Die Lambda-Funktion sollte nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihren Funktionscode ermöglichen kann.

Abhilfe

Um dieses Problem zu beheben, müssen Sie die ressourcenbasierte Richtlinie Ihrer Funktion aktualisieren, um Berechtigungen zu entfernen oder die Bedingung hinzuzufügen.

AWS:SourceAccount Sie können die ressourcenbasierte Richtlinie nur über die Lambda-API oder aktualisieren. **AWS CLI**

[Überprüfen Sie zunächst die ressourcenbasierte Richtlinie auf](#) der Lambda-Konsole. Identifizieren Sie die Richtlinienaussage, deren Principal Feldwerte die Richtlinie öffentlich machen, z. B. oder. "*" { "AWS": "*" }

Sie können die Richtlinie nicht von der Konsole aus bearbeiten. Um der Funktion Berechtigungen zu entziehen, führen Sie den [remove-permission](#) Befehl über den aus AWS CLI.

```
$ aws lambda remove-permission --function-name <function-name> --statement-id <statement-id>
```

<function-name> Ersetzen Sie durch den Namen der Lambda-Funktion und *<statement-id>* durch die Anweisungs-ID (Sid) der Anweisung, die Sie entfernen möchten.

[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), NIST.800-53.R5 SI-2 (5), PCI DSS v4.0.1/12.3.4

Kategorie: Schutz > Sichere Entwicklung

Schweregrad: Mittel

Ressourcentyp: AWS::Lambda::Function

AWS Config -Regel: [lambda-function-settings-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- runtime: dotnet8, java21, java17, java11, java8.al2, nodejs22.x, nodejs20.x, nodejs18.x, python3.13, python3.12, python3.11, python3.10, python3.9, ruby3.4, ruby3.3, ruby3.2 (nicht anpassbar)

Dieses Steuerelement prüft, ob die Laufzeiteinstellungen der AWS Lambda Funktionen mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Die Steuerung schlägt fehl, wenn die Lambda-Funktion keine unterstützte Laufzeit verwendet, wie im Abschnitt Parameter angegeben. Security Hub ignoriert Funktionen mit dem PakettypImage.

Lambda-Laufzeiten basieren auf einer Kombination aus Betriebssystem, Programmiersprache und Softwarebibliotheken, die Wartungs- und Sicherheitsupdates unterliegen. Wenn eine Laufzeitkomponente für Sicherheitsupdates nicht mehr unterstützt wird, hat Lambda die Laufzeit als veraltet eingestuft. Auch wenn Sie keine Funktionen erstellen können, die die veraltete Runtime verwenden, ist die Funktion dennoch für die Verarbeitung von Aufrufereignissen verfügbar.

Wir empfehlen sicherzustellen, dass Ihre Lambda-Funktionen aktuell sind und keine veralteten Laufzeitumgebungen verwenden. Eine Liste der unterstützten Laufzeiten finden Sie unter [Lambda-Laufzeiten im AWS Lambda Developer Guide](#).

Abhilfe

Weitere Informationen zu unterstützten Laufzeiten und Zeitplänen für veraltete Versionen finden Sie unter [Runtime Deprecation](#) Policy im Developer Guide.AWS Lambda Wenn Sie Ihre Laufzeiten auf die neueste Version migrieren, folgen Sie der Syntax und Anleitung der Herausgeber der Sprache. Wir empfehlen außerdem, [Runtime-Updates](#) zu installieren, um das Risiko einer Beeinträchtigung Ihrer Workloads zu verringern, falls es in seltenen Fällen zu einer Inkompatibilität einer Runtime-Version kommen sollte.

[Lambda.3] Lambda-Funktionen sollten sich in einer VPC befinden

Verwandte Anforderungen: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-3,, (11)

NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (16) NIST.800-53.r5 AC-6, (20) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Niedrig

Ressourcentyp: AWS::Lambda::Function

AWS Config Regel: [lambda-inside-vpc](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Lambda-Funktion in einer Virtual Private Cloud (VPC) bereitgestellt ist. Die Steuerung schlägt fehl, wenn die Lambda-Funktion nicht in einer VPC bereitgestellt wird. Security Hub bewertet die Konfiguration des VPC-Subnetz-Routings nicht, um die öffentliche Erreichbarkeit zu ermitteln. Möglicherweise werden fehlgeschlagene Ergebnisse für Lambda @Edge -Ressourcen angezeigt.

Die Bereitstellung von Ressourcen in einer VPC verbessert die Sicherheit und Kontrolle über Netzwerkkonfigurationen. Solche Bereitstellungen bieten auch Skalierbarkeit und hohe Fehlertoleranz über mehrere Availability Zones hinweg. Sie können VPC-Bereitstellungen an unterschiedliche Anwendungsanforderungen anpassen.

Abhilfe

Informationen zur Konfiguration einer vorhandenen Funktion zum Herstellen einer Verbindung zu privaten Subnetzen in Ihrer VPC finden Sie unter [Konfiguration des VPC-Zugriffs im AWS Lambda Entwicklerhandbuch](#). Wir empfehlen, mindestens zwei private Subnetze für hohe Verfügbarkeit und mindestens eine Sicherheitsgruppe auszuwählen, die die Konnektivitätsanforderungen der Funktion erfüllt.

[Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::Lambda::Function`

AWS Config -Regel: [lambda-vpc-multi-az-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>availabilityZones</code>	Mindestanzahl von Availability Zones	Enum	2, 3, 4, 5, 6	2

Dieses Steuerelement prüft, ob eine AWS Lambda Funktion, die eine Verbindung zu einer Virtual Private Cloud (VPC) herstellt, in mindestens der angegebenen Anzahl von Availability Zone (AZs) betrieben wird. Die Steuerung schlägt fehl, wenn die Funktion nicht in mindestens der angegebenen Anzahl von AZs funktioniert. Sofern Sie keinen benutzerdefinierten Parameterwert für die Mindestanzahl von angeben AZs, verwendet Security Hub den Standardwert AZs 2.

Die Bereitstellung mehrerer Ressourcen AZs ist eine AWS bewährte Methode, um eine hohe Verfügbarkeit innerhalb Ihrer Architektur sicherzustellen. Verfügbarkeit ist eine zentrale Säule des dreifachen Sicherheitsmodells für Vertraulichkeit, Integrität und Verfügbarkeit. Alle Lambda-Funktionen, die eine Verbindung zu einer VPC herstellen, sollten über eine Multi-AZ-Bereitstellung verfügen, um sicherzustellen, dass eine einzelne Ausfallzone nicht zu einer vollständigen Betriebsunterbrechung führt.

Abhilfe

Wenn Sie Ihre Funktion so konfigurieren, dass sie eine Verbindung zu einer VPC in Ihrem Konto herstellt, geben Sie mehrere Subnetze an, um eine hohe AZs Verfügbarkeit zu gewährleisten. Anweisungen finden Sie unter [Konfiguration des VPC-Zugriffs](#) im AWS Lambda Entwicklerhandbuch.

Lambda führt automatisch mehrere Funktionen aus, AZs um sicherzustellen, dass es für die Verarbeitung von Ereignissen im Falle einer Serviceunterbrechung in einer einzelnen Zone verfügbar ist.

[Lambda.6] Lambda-Funktionen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Lambda::Function`

AWS Config Regel: `tagged-lambda-function` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob eine AWS Lambda Funktion über Tags mit den spezifischen Tasten verfügt, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn die Funktion keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Funktion mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `aws:*` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie

außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Lambda-Funktion finden Sie unter [Verwenden von Tags für Lambda-Funktionen](#) im AWS Lambda Entwicklerhandbuch.

[Lambda.7] Bei Lambda-Funktionen sollte aktives Tracing aktiviert sein AWS X-Ray

Verwandte Anforderungen: NIST.800-53.r5 CA-7

Kategorie: Identifizieren > Protokollierung

Schweregrad: Niedrig

Art der Ressource: AWS::Lambda::Function

AWS Config -Regel: [lambda-function-xray-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob das aktive Tracing mit für eine AWS Lambda Funktion aktiviert AWS X-Ray ist. Die Steuerung schlägt fehl, wenn das aktive Tracing mit X-Ray für die Lambda-Funktion deaktiviert ist.

AWS X-Ray kann AWS Lambda Funktionen zur Nachverfolgung und Überwachung bereitstellen, wodurch Zeit und Mühe beim Debuggen und Bedienen von Lambda-Funktionen eingespart werden können. Es kann Ihnen helfen, Fehler zu diagnostizieren und Leistungsengpässe, Verlangsamungen und Timeouts zu identifizieren, indem es die Latenz für Lambda-Funktionen aufschlüsselt. Es kann auch bei Datenschutz- und Compliance-Anforderungen helfen. Wenn Sie die aktive Ablaufverfolgung für eine Lambda-Funktion aktivieren, bietet X-Ray einen ganzheitlichen Überblick über den Datenfluss und die Verarbeitung innerhalb der Lambda-Funktion, sodass Sie potenzielle Sicherheitslücken oder nicht konforme Datenverarbeitungspraktiken identifizieren können. Diese Transparenz kann Ihnen helfen, Datenintegrität und Vertraulichkeit zu wahren und die Einhaltung relevanter Vorschriften zu gewährleisten.

Note

AWS X-Ray Die Ablaufverfolgung wird derzeit nicht für Lambda-Funktionen mit Amazon Managed Streaming for Apache Kafka (Amazon MSK), selbstverwaltetem Apache Kafka, Amazon MQ mit ActiveMQ und RabbitMQ oder Amazon DocumentDB DocumentDB-Ereignisquellenzuordnungen unterstützt.

Abhilfe

Informationen zur Aktivierung von Active Tracing für eine AWS Lambda Funktion finden Sie unter [Visualize Lambda function invocations using AWS X-Ray](#) im Developer Guide.AWS Lambda

Security Hub-Steuerelemente für Macie

Diese AWS Security Hub Kontrollen bewerten den Amazon Macie-Service.

Diese Kontrollen sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[Macie.1] Amazon Macie sollte aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-7, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 SA-8 (19) NIST.800-53.r5 RA-5, NIST.800-53.R5 SI-4

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Mittel

Art der Ressource: AWS:::Account

AWS Config -Regel: [macie-status-check](#)

Art des Zeitplans: Periodisch

Diese Kontrolle prüft, ob Amazon Macie für ein Konto aktiviert ist. Die Kontrolle schlägt fehl, wenn Macie für das Konto nicht aktiviert ist.

Amazon Macie erkennt sensible Daten mithilfe von maschinellem Lernen und Musterabgleich, bietet Einblick in Datensicherheitsrisiken und ermöglicht automatisierten Schutz vor diesen Risiken. Macie bewertet Ihre Amazon Simple Storage Service (Amazon S3) -Buckets automatisch und kontinuierlich im Hinblick auf Sicherheit und Zugriffskontrolle und generiert Ergebnisse, um Sie über potenzielle Probleme mit der Sicherheit oder dem Datenschutz Ihrer Amazon S3-Daten zu informieren. Macie automatisiert auch die Erkennung und Meldung sensibler Daten, wie z. B. personenbezogener Daten (PII), um Ihnen ein besseres Verständnis der Daten zu vermitteln, die Sie in Amazon S3 speichern. Weitere Informationen finden Sie im [Amazon Macie Macie-Benutzerhandbuch](#).

Abhilfe

Informationen zur Aktivierung von Macie finden Sie unter [Macie aktivieren](#) im Amazon Macie Macie-Benutzerhandbuch.

[Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-7, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 SA-8 (19) NIST.800-53.r5 RA-5, NIST.800-53.R5 SI-4

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Hoch

Art der Ressource: AWS:::Account

AWS Config -Regel: [macie-auto-sensitive-data-discovery-check](#)

Art des Zeitplans: Periodisch

Dieses Steuerelement prüft, ob die automatische Erkennung sensibler Daten für ein Amazon Macie-Administratorkonto aktiviert ist. Die Kontrolle schlägt fehl, wenn die automatische Erkennung sensibler Daten für ein Macie-Administratorkonto nicht aktiviert ist. Dieses Steuerelement gilt nur für Administratorkonten.

Macie automatisiert die Erkennung und Meldung sensibler Daten, wie z. B. persönlich identifizierbare Informationen (PII), in Amazon Simple Storage Service (Amazon S3) -Buckets. Mit der automatisierten Erkennung sensibler Daten bewertet Macie kontinuierlich Ihr Bucket-Inventar und verwendet Stichprobenverfahren, um repräsentative S3-Objekte aus Ihren Buckets zu identifizieren und auszuwählen. Macie analysiert dann die ausgewählten Objekte und untersucht sie auf sensible Daten. Im Verlauf der Analysen aktualisiert Macie Statistiken, Inventardaten und andere Informationen, die es zu Ihren S3-Daten bereitstellt. Macie generiert auch Ergebnisse, um gefundene sensible Daten zu melden.

Abhilfe

Informationen zum Erstellen und Konfigurieren automatisierter Discovery-Jobs für sensible Daten zur Analyse von Objekten in S3-Buckets finden Sie unter [Konfiguration der automatisierten Erkennung sensibler Daten für Ihr Konto](#) im Amazon Macie Macie-Benutzerhandbuch.

Security Hub-Steuerelemente für Amazon MSK

Diese AWS Security Hub Kontrollen bewerten den Service und die Ressourcen von Amazon Managed Streaming for Apache Kafka (Amazon MSK). Die Steuerelemente sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 3, 3 (NIST.800-53.r5 SC-23), NIST.800-53.r5 SC-2 (4), NIST.800-53.r5 SC-7 (1), NIST.800-53.r5 SC-8 (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 PCI DSS v4.0.1/4.2.1

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: AWS::MSK::Cluster

AWS Config -Regel: [msk-in-cluster-node-require-tls](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob ein Amazon MSK-Cluster bei der Übertragung mit HTTPS (TLS) zwischen den Broker-Knoten des Clusters verschlüsselt ist. Die Steuerung schlägt fehl, wenn die Klartext-Kommunikation für eine Cluster-Broker-Knotenverbindung aktiviert ist.

HTTPS bietet eine zusätzliche Sicherheitsebene, da TLS für die Übertragung von Daten verwendet wird, und kann dazu beitragen, potenzielle Angreifer daran zu hindern, person-in-the-middle Netzwerkverkehr mit oder ähnlichen Angriffen zu belauschen oder zu manipulieren. Standardmäßig verschlüsselt Amazon MSK Daten bei der Übertragung mit TLS. Sie können diese Standardeinstellung jedoch bei der Erstellung des Clusters überschreiben. Wir empfehlen die Verwendung verschlüsselter Verbindungen über HTTPS (TLS) für Broker-Knotenverbindungen.

Abhilfe

Informationen zur Aktualisierung der Verschlüsselungseinstellungen für einen Amazon MSK-Cluster finden Sie unter [Aktualisieren der Sicherheitseinstellungen eines Clusters](#) im Amazon Managed Streaming for Apache Kafka Developer Guide.

[MSK.2] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-2

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Art der Ressource: AWS::MSK::Cluster

AWS Config -Regel: [msk-enhanced-monitoring-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für einen Amazon MSK-Cluster eine erweiterte Überwachung konfiguriert ist, die durch eine Überwachungsebene von mindestens PER_TOPIC_PER_BROKER angegeben wird. Die Steuerung schlägt fehl, wenn die Überwachungsebene für den Cluster auf DEFAULT oder PER_BROKER gesetzt ist.

Die PER_TOPIC_PER_BROKER Überwachungsebene bietet detailliertere Einblicke in die Leistung Ihres MSK-Clusters und bietet auch Metriken zur Ressourcennutzung, z. B. zur

CPU- und Speicherauslastung. Auf diese Weise können Sie Leistungsengpässe und Ressourcennutzungsmuster für einzelne Themen und Broker identifizieren. Diese Transparenz kann wiederum die Leistung Ihrer Kafka-Broker optimieren.

Abhilfe

Gehen Sie wie folgt vor, um die erweiterte Überwachung für einen MSK-Cluster zu konfigurieren:

1. Die Amazon MSK-Konsole zu [https://console.aws.amazon.com/msk/Hause öffnen? region=us-east-1#/home/](https://console.aws.amazon.com/msk/Hause%20öffnen?region=us-east-1#/home/).
2. Klicken Sie im Navigationsbereich auf Cluster. Wählen Sie dann einen Cluster aus.
3. Wählen Sie für Aktion die Option Überwachung bearbeiten aus.
4. Wählen Sie die Option für Erweiterte Überwachung auf Themenebene aus.
5. Wählen Sie Änderungen speichern aus.

Weitere Informationen zu Überwachungsebenen finden Sie unter [Amazon MSK-Metriken für die Überwachung von Standard-Brokern mit CloudWatch](#) im Amazon Managed Streaming for Apache Kafka Developer Guide.

[MSK.3] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden

Verwandte Anforderungen: PCI DSS v4.0.1/4.2.1

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: AWS::KafkaConnect::Connector

AWS Config Regel: msk-connect-connector-encrypted (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon MSK Connect-Konnektor während der Übertragung verschlüsselt ist. Diese Kontrolle schlägt fehl, wenn der Connector bei der Übertragung nicht verschlüsselt wird.

Daten während der Übertragung beziehen sich auf Daten, die von einem Ort an einen anderen übertragen werden, z. B. zwischen Knoten in Ihrem Cluster oder zwischen Ihrem Cluster und Ihrer Anwendung. Daten können über das Internet oder innerhalb eines privaten Netzwerks übertragen werden. Durch die Verschlüsselung von Daten während der Übertragung wird das Risiko verringert, dass ein nicht autorisierter Benutzer den Netzwerkverkehr abhören kann.

Abhilfe

Sie können die Verschlüsselung bei der Übertragung aktivieren, wenn Sie einen MSK Connect-Connector erstellen. Sie können die Verschlüsselungseinstellungen nach dem Erstellen eines Connectors nicht ändern. Weitere Informationen finden Sie unter [Create a Connector](#) im Amazon Managed Streaming for Apache Kafka Developer Guide.

[MSK.4] Bei MSK-Clustern sollte der öffentliche Zugriff deaktiviert sein

Kategorie: Schützen > Sichere Zugriffsverwaltung > Ressource nicht öffentlich zugänglich

Schweregrad: Kritisch

Art der Ressource: `AWS::MSK::Cluster`

AWS Config -Regel: [msk-cluster-public-access-disabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der öffentliche Zugriff für einen Amazon MSK-Cluster deaktiviert ist. Die Kontrolle schlägt fehl, wenn der öffentliche Zugriff für den MSK-Cluster aktiviert ist.

Standardmäßig können Clients nur dann auf einen Amazon MSK-Cluster zugreifen, wenn sie sich in derselben VPC wie der Cluster befinden. Die gesamte Kommunikation zwischen Kafka-Clients und einem MSK-Cluster ist standardmäßig privat und Streaming-Daten werden nicht über das Internet übertragen. Wenn ein MSK-Cluster jedoch so konfiguriert ist, dass er öffentlichen Zugriff zulässt, kann jeder im Internet eine Verbindung zu Apache Kafka-Brokern herstellen, die innerhalb des Clusters ausgeführt werden. Dies kann zu Problemen wie unberechtigtem Zugriff, Datenschutzverletzungen oder der Ausnutzung von Sicherheitslücken führen. Wenn Sie den Zugriff auf einen Cluster einschränken, indem Sie Authentifizierungs- und Autorisierungsmaßnahmen vorschreiben, können Sie dazu beitragen, vertrauliche Informationen zu schützen und die Integrität Ihrer Ressourcen aufrechtzuerhalten.

Abhilfe

Informationen zur Verwaltung des öffentlichen Zugriffs auf einen Amazon MSK-Cluster finden Sie unter [Aktivieren des öffentlichen Zugriffs auf einen von MSK bereitgestellten Cluster](#) im Amazon Managed Streaming for Apache Kafka Developer Guide.

[MSK.5] Bei MSK-Konnektoren sollte die Protokollierung aktiviert sein

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS::KafkaConnect::Connector

AWS Config -Regel: [msk-connect-connector-logging-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Protokollierung für einen Amazon MSK-Connector aktiviert ist. Die Steuerung schlägt fehl, wenn die Protokollierung für den MSK-Connector deaktiviert ist.

Amazon MSK-Konnektoren integrieren externe Systeme und Amazon-Services mit Apache Kafka, indem sie kontinuierlich Streaming-Daten aus einer Datenquelle in einen Apache Kafka-Cluster oder kontinuierlich Daten aus einem Cluster in eine Datensenke kopieren. MSK Connect kann Protokollereignisse schreiben, die beim Debuggen eines Connectors helfen können. Wenn Sie einen Connector erstellen, können Sie null oder mehr der folgenden Protokollziele angeben: Amazon CloudWatch Logs, Amazon S3 und Amazon Data Firehose.

Note

Vertrauliche Konfigurationswerte können in Konnektor-Protokollen erscheinen, wenn ein Plugin diese Werte nicht als Secret definiert. Kafka Connect behandelt undefinierte Konfigurationswerte genauso wie jeden anderen Klartext-Wert.

Abhilfe

Um die Protokollierung für einen vorhandenen Amazon MSK-Connector zu aktivieren, müssen Sie den Connector mit der entsprechenden Protokollierungskonfiguration neu erstellen. Informationen zu

Konfigurationsoptionen finden Sie unter [Logging for MSK Connect](#) im Amazon Managed Streaming for Apache Kafka Developer Guide.

[MSK.6] MSK-Cluster sollten den nicht authentifizierten Zugriff deaktivieren

Kategorie: Schützen > Sichere Zugriffsverwaltung > Passwortlose Authentifizierung

Schweregrad: Mittel

Art der Ressource: `AWS::MSK::Cluster`

AWS Config -Regel: [msk-unrestricted-access-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob der nicht authentifizierte Zugriff für einen Amazon MSK-Cluster aktiviert ist. Die Kontrolle schlägt fehl, wenn der nicht authentifizierte Zugriff für den MSK-Cluster aktiviert ist.

Amazon MSK unterstützt Client-Authentifizierungs- und Autorisierungsmechanismen, um den Zugriff auf einen Cluster zu kontrollieren. Diese Mechanismen überprüfen die Identität der Clients, die sich mit dem Cluster verbinden, und bestimmen, welche Aktionen Clients ausführen können. Ein MSK-Cluster kann so konfiguriert werden, dass er nicht authentifizierten Zugriff ermöglicht, sodass jeder Client mit Netzwerkkonnektivität Kafka-Themen veröffentlichen und abonnieren kann, ohne Anmeldeinformationen angeben zu müssen. Das Ausführen eines MSK-Clusters ohne Authentifizierung verstößt gegen das Prinzip der geringsten Rechte und kann den Cluster unberechtigtem Zugriff aussetzen. Es kann jedem Client ermöglichen, auf Daten in Kafka-Themen zuzugreifen, diese zu ändern oder zu löschen, was möglicherweise zu Datenschutzverletzungen, unbefugten Datenänderungen oder Dienstunterbrechungen führen kann. Wir empfehlen, Authentifizierungsmechanismen wie IAM-Authentifizierung, SASL/SCRAM oder Mutual TLS zu aktivieren, um eine angemessene Zugriffskontrolle zu gewährleisten und die Einhaltung der Sicherheitsbestimmungen zu gewährleisten.

Abhilfe

Informationen zum Ändern der Authentifizierungseinstellungen für einen Amazon MSK-Cluster finden Sie in den folgenden Abschnitten des Amazon Managed Streaming for Apache Kafka Developer Guide: [Sicherheitseinstellungen eines Amazon MSK-Clusters aktualisieren und Authentifizierung und Autorisierung für Apache Kafka](#). APIs

Security Hub-Steuerelemente für Amazon MQ

Diese AWS Security Hub Kontrollen bewerten den Service und die Ressourcen von Amazon MQ.

Diese Kontrollen sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch

Verwandte Anforderungen: NIST.800-53.R5 AU-2, NIST.800-53.R5 AU-3, NIST.800-53.R5 AU-12, NIST.800-53.R5 SI-4, PCI DSS v4.0.1/10.3.3

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS::AmazonMQ::Broker

AWS Config -Regel: [mq-cloudwatch-audit-log-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon MQ ActiveMQ-Broker Auditprotokolle an Amazon Logs streamt. CloudWatch Die Kontrolle schlägt fehl, wenn der Broker keine Auditprotokolle in Logs streamt. CloudWatch

Durch die Veröffentlichung von CloudWatch ActiveMQ-Broker-Protokollen in Logs können Sie CloudWatch Alarme und Metriken erstellen, die die Sichtbarkeit sicherheitsrelevanter Informationen erhöhen.

Abhilfe

Informationen zum Streamen von CloudWatch ActiveMQ-Broker-Protokollen in Logs finden Sie unter [Konfiguration von Amazon MQ für ActiveMQ-Protokolle im Amazon MQ Developer Guide](#).

[MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 CM-3, NIST.800-53.R5 SI-2, PCI DSS v4.0.1/6.3.3

Kategorie: Identifizieren > Schwachstellen-, Patch- und Versionsverwaltung

Schweregrad: Niedrig

Art der Ressource: AWS::AmazonMQ::Broker

AWS Config -Regel: [mq-auto-minor-version-upgrade-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob bei einem Amazon MQ-Broker das automatische Upgrade für Nebenversionen aktiviert ist. Die Kontrolle schlägt fehl, wenn der Broker das automatische Upgrade der Nebenversion nicht aktiviert hat.

Da Amazon MQ neue Broker-Engine-Versionen veröffentlicht und unterstützt, sind die Änderungen abwärtskompatibel mit einer vorhandenen Anwendung und verwerfen keine bestehenden Funktionen. Automatische Versionsupdates der Broker Engine schützen Sie vor Sicherheitsrisiken, helfen bei der Behebung von Fehlern und verbessern die Funktionalität.

 Note

Wenn der Broker, der mit dem automatischen Upgrade einer Nebenversion verknüpft ist, seinen neuesten Patch installiert hat und nicht mehr unterstützt wird, müssen Sie für das Upgrade manuelle Maßnahmen ergreifen.

Abhilfe

Informationen zur Aktivierung des automatischen Upgrades der Nebenversion für einen MQ-Broker finden Sie unter [Automatisches Upgrade der Nebenversion der Engine](#) im Amazon MQ Developer Guide.

[MQ.4] Amazon MQ-Broker sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::AmazonMQ::Broker

AWS Config Regel: tagged-amazonmq-broker (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob ein Amazon MQ-Broker über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn der Broker keine Tag-Schlüssel hat oder wenn er nicht über alle im Parameter `requiredTagKeys` angegebenen Schlüssel verfügt. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Broker mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `aws:` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Amazon MQ-Broker finden Sie unter [Tagging resources](#) im Amazon MQ Developer Guide.

[MQ.5] ActiveMQ-Broker sollten den Aktiv-/Standby-Bereitstellungsmodus verwenden

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Niedrig

Art der Ressource: AWS::AmazonMQ::Broker

AWS Config -Regel: [mq-active-deployment-mode](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der Bereitstellungsmodus für einen Amazon MQ ActiveMQ-Broker auf Aktiv/Standby eingestellt ist. Die Steuerung schlägt fehl, wenn ein Single-Instance-Broker (standardmäßig aktiviert) als Bereitstellungsmodus festgelegt ist.

Die Aktiv-/Standby-Bereitstellung bietet Hochverfügbarkeit für Ihre Amazon MQ ActiveMQ-Broker in einem. AWS-Region Der Aktiv-/Standby-Bereitstellungsmodus umfasst zwei Broker-Instances in zwei verschiedenen Availability Zones, die in einem redundanten Paar konfiguriert sind. Diese Broker kommunizieren synchron mit Ihrer Anwendung, wodurch Ausfallzeiten und Datenverluste im Falle eines Fehlers reduziert werden können.

Abhilfe

Informationen zum Erstellen eines neuen ActiveMQ-Brokers mit aktivem Bereitstellungsmodus finden Sie unter [Erstellen und Konfigurieren eines ActiveMQ-Brokers im Amazon MQ Developer Guide](#). Wählen Sie für den Bereitstellungsmodus die Option Active/Standby-Broker. Sie können den Bereitstellungsmodus für einen vorhandenen Broker nicht ändern. Stattdessen müssen Sie einen neuen Broker erstellen und die Einstellungen aus dem alten Broker kopieren.

[MQ.6] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Niedrig

Art der Ressource: AWS::AmazonMQ::Broker

AWS Config -Regel: [mq-rabbit-deployment-mode](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der Bereitstellungsmodus für einen Amazon MQ RabbitMQ-Broker auf Cluster-Bereitstellung eingestellt ist. Die Steuerung schlägt fehl, wenn ein Single-Instance-Broker (standardmäßig aktiviert) als Bereitstellungsmodus festgelegt ist.

Die Cluster-Bereitstellung bietet Hochverfügbarkeit für Ihre Amazon MQ RabbitMQ-Broker in einem AWS-Region. Die Cluster-Bereitstellung ist eine logische Gruppierung von drei RabbitMQ-Broker-Knoten, von denen jeder über ein eigenes Amazon Elastic Block Store (Amazon EBS) -Volume und einen gemeinsamen Status verfügt. Die Cluster-Bereitstellung stellt sicher, dass Daten auf alle Knoten im Cluster repliziert werden, wodurch Ausfallzeiten und Datenverluste im Falle eines Fehlers reduziert werden können.

Abhilfe

Informationen zum Erstellen eines neuen RabbitMQ-Brokers mit Cluster-Bereitstellungsmodus finden Sie unter [Erstellen und Herstellen einer Verbindung zu einem RabbitMQ-Broker im Amazon MQ Developer Guide](#). Wählen Sie für den Bereitstellungsmodus die Option Cluster-Bereitstellung. Sie

können den Bereitstellungsmodus für einen vorhandenen Broker nicht ändern. Stattdessen müssen Sie einen neuen Broker erstellen und die Einstellungen aus dem alten Broker kopieren.

Security Hub-Steuerungen für Neptune

Diese AWS Security Hub Kontrollen bewerten den Service und die Ressourcen von Amazon Neptune.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 (1), (10), NIST.800-53.r5 SC-2 NIST.800-53.R5 SI-7 NIST.800-53.r5 SC-7 (6)

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: AWS::RDS::DBCluster

AWS Config -Regel: [neptune-cluster-encrypted](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Neptune-DB-Cluster im Ruhezustand verschlüsselt ist. Die Steuerung schlägt fehl, wenn ein Neptune-DB-Cluster im Ruhezustand nicht verschlüsselt ist.

Daten im Ruhezustand beziehen sich auf alle Daten, die für einen beliebigen Zeitraum in einem persistenten, nichtflüchtigen Speicher gespeichert werden. Durch Verschlüsselung können Sie die Vertraulichkeit solcher Daten schützen und so das Risiko verringern, dass ein unberechtigter Benutzer darauf zugreifen kann. Die Verschlüsselung Ihrer Neptune-DB-Cluster schützt Ihre Daten und Metadaten vor unbefugtem Zugriff. Es erfüllt auch die Compliance-Anforderungen für die data-at-rest Verschlüsselung von Produktionsdateisystemen.

Abhilfe

Sie können die Verschlüsselung im Ruhezustand aktivieren, wenn Sie einen Neptune-DB-Cluster erstellen. Sie können die Verschlüsselungseinstellungen nach dem Erstellen eines Clusters nicht

ändern. Weitere Informationen finden Sie unter [Encrypting Neptune resources at rest im Neptune-Benutzerhandbuch](#).

[Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-6(5), NIST.800-53.r5 AU-7(1), NIST.800-53.r5 AU-9(7), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-20, NIST.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-4 (5), NIST.800-53.R5 SI-7 (8), PCI DSS v4.0.1/10.3.3

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS::RDS::DBCluster

AWS Config -Regel: [neptune-cluster-cloudwatch-log-export-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob ein Neptune-DB-Cluster Audit-Logs in Amazon CloudWatch Logs veröffentlicht. Die Steuerung schlägt fehl, wenn ein Neptune-DB-Cluster keine Audit-Logs in Logs veröffentlicht. CloudWatch EnableCloudWatchLogsExports sollte auf eingestellt sein. Audit

Amazon Neptune und Amazon CloudWatch sind integriert, sodass Sie Leistungskennzahlen sammeln und analysieren können. Neptune sendet automatisch Messwerte an Alarme CloudWatch und unterstützt CloudWatch diese auch. Audit-Logs sind hochgradig anpassbar. Wenn Sie eine Datenbank prüfen, kann jeder Vorgang an den Daten überwacht und in einem Audit-Trail protokolliert werden, einschließlich Informationen darüber, auf welchen Datenbankcluster zugegriffen wird und wie. Wir empfehlen, diese Protokolle an zu senden, CloudWatch um Ihnen bei der Überwachung Ihrer Neptune-DB-Cluster zu helfen.

Abhilfe

Informationen zum Veröffentlichen von Neptune-Audit-Logs in CloudWatch Logs finden Sie unter [Neptune-Logs in Amazon CloudWatch Logs veröffentlichen](#) im Neptune-Benutzerhandbuch. Wählen Sie im Abschnitt Protokollexporte die Option Audit aus.

[Neptune.3] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3, (21), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (11), (16) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), (4), NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS NIST.800-53.r5 SC-7 v4.0.1/1.4.4 NIST.800-53.r5 SC-7

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Kritisch

Art der Ressource: AWS::RDS::DBClusterSnapshot

AWS Config -Regel: [neptune-cluster-snapshot-public-prohibited](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein manueller Neptune-DB-Cluster-Snapshot öffentlich ist. Die Steuerung schlägt fehl, wenn ein manueller Neptune-DB-Cluster-Snapshot öffentlich ist.

Ein manueller Snapshot eines Neptune-DB-Clusters sollte nicht öffentlich sein, es sei denn, dies ist beabsichtigt. Wenn Sie einen unverschlüsselten manuellen Snapshot als öffentlich freigeben, ist der Snapshot für alle verfügbar. AWS-Konten Öffentliche Snapshots können zu einer unbeabsichtigten Offenlegung von Daten führen.

Abhilfe

Informationen zum Entfernen des öffentlichen Zugriffs für manuelle Neptune-DB-Cluster-Snapshots finden Sie unter [Freigeben eines DB-Cluster-Snapshots](#) im Neptune-Benutzerhandbuch.

[Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), (2) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5

Kategorie: Schützen > Datenschutz > Schutz vor Datenlöschung

Schweregrad: Niedrig

Art der Ressource: AWS::RDS::DBCluster

AWS Config -Regel: [neptune-cluster-deletion-protection-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob in einem Neptune-DB-Cluster der Löschschutz aktiviert ist. Die Steuerung schlägt fehl, wenn für einen Neptune-DB-Cluster kein Löschschutz aktiviert ist.

Die Aktivierung des Cluster-Löschschutzes bietet eine zusätzliche Schutzebene vor dem versehentlichen Löschen von Datenbanken oder vor dem Löschen durch einen nicht autorisierten Benutzer. Ein Neptune-DB-Cluster kann nicht gelöscht werden, solange der Löschschutz aktiviert ist. Sie müssen zuerst den Löschschutz deaktivieren, bevor eine Löschanfrage erfolgreich sein kann.

Abhilfe

Informationen zum Aktivieren des Löschschutzes für einen vorhandenen Neptune-DB-Cluster finden Sie unter [Ändern des DB-Clusters mithilfe der Konsole, der CLI und der API](#) im Amazon Aurora Aurora-Benutzerhandbuch.

[Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 SI-12

Kategorie: Wiederherstellung > Ausfallsicherheit > Backups aktiviert

Schweregrad: Mittel

Art der Ressource: AWS::RDS::DBCluster

AWS Config -Regel: [neptune-cluster-backup-retention-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Standardwert	
minimumBackupRetentionPeriod	Minimale Aufbewahrungsdauer für Backups in Tagen	Ganzzahl	7 auf 35	7	

Dieses Steuerelement prüft, ob in einem Neptune-DB-Cluster automatische Backups aktiviert sind und ob die Aufbewahrungsfrist für Backups größer oder gleich dem angegebenen Zeitraum ist. Die Kontrolle schlägt fehl, wenn Backups für den Neptune-DB-Cluster nicht aktiviert sind oder wenn die Aufbewahrungszeit kürzer als der angegebene Zeitraum ist. Sofern Sie keinen benutzerdefinierten Parameterwert für die Aufbewahrungsdauer von Backups angeben, verwendet Security Hub einen Standardwert von 7 Tagen.

Backups helfen Ihnen, sich nach einem Sicherheitsvorfall schneller zu erholen und die Widerstandsfähigkeit Ihrer Systeme zu stärken. Durch die Automatisierung von Backups für Ihre Neptune-DB-Cluster können Sie Ihre Systeme zu einem bestimmten Zeitpunkt wiederherstellen und Ausfallzeiten und Datenverluste minimieren.

Abhilfe

Informationen zur Aktivierung automatisierter Backups und zur Festlegung einer Aufbewahrungsfrist für Backups für Ihre Neptune-DB-Cluster finden Sie unter [Automatisierte Backups aktivieren](#) im Amazon RDS-Benutzerhandbuch. Wählen Sie für den Aufbewahrungszeitraum für Backup einen Wert größer oder gleich 7.

[Neptune.6] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), (10), NIST.800-53.r5 SC-7 (18) NIST.800-53.r5 SC-7

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: AWS::RDS::DBClusterSnapshot

AWS Config -Regel: [neptune-cluster-snapshot-encrypted](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Neptune-DB-Cluster-Snapshot im Ruhezustand verschlüsselt ist. Die Steuerung schlägt fehl, wenn ein Neptune-DB-Cluster im Ruhezustand nicht verschlüsselt ist.

Daten im Ruhezustand beziehen sich auf alle Daten, die für einen beliebigen Zeitraum in einem persistenten, nichtflüchtigen Speicher gespeichert werden. Durch Verschlüsselung können Sie die Vertraulichkeit solcher Daten schützen und so das Risiko verringern, dass ein nicht autorisierter Benutzer darauf zugreifen kann. Daten in Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden, um eine zusätzliche Sicherheitsebene zu gewährleisten.

Abhilfe

Sie können einen vorhandenen Neptune-DB-Cluster-Snapshot nicht verschlüsseln. Stattdessen müssen Sie den Snapshot in einem neuen DB-Cluster wiederherstellen und die Verschlüsselung auf dem Cluster aktivieren. Sie können einen verschlüsselten Snapshot aus dem verschlüsselten Cluster erstellen. Anweisungen finden Sie unter [Wiederherstellung aus einem DB-Cluster-Snapshot](#) und [Erstellen eines DB-Cluster-Snapshots in Neptune im Neptune-Benutzerhandbuch](#).

[Neptune.7] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1), (15), NIST.800-53.r5 AC-3 (NIST.800-53.r5 AC-37), NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6

Kategorie: Schützen > Sichere Zugriffsverwaltung > Passwortlose Authentifizierung

Schweregrad: Mittel

Art der Ressource: AWS::RDS::DBCluster

AWS Config -Regel: [neptune-cluster-iam-database-authentication](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob in einem Neptune-DB-Cluster die IAM-Datenbankauthentifizierung aktiviert ist. Die Steuerung schlägt fehl, wenn die IAM-Datenbankauthentifizierung für einen Neptune-DB-Cluster nicht aktiviert ist.

Die IAM-Datenbankauthentifizierung für Amazon Neptune Neptune-Datenbankcluster macht das Speichern von Benutzeranmeldeinformationen in der Datenbankkonfiguration überflüssig, da die Authentifizierung extern mithilfe von IAM verwaltet wird. Wenn die IAM-Datenbankauthentifizierung aktiviert ist, muss jede Anfrage mit Signature Version 4 signiert werden. AWS

Abhilfe

Standardmäßig ist die IAM-Datenbankauthentifizierung deaktiviert, wenn Sie einen Neptune-DB-Cluster erstellen. Informationen zur [Aktivierung finden Sie unter Aktivieren der IAM-Datenbankauthentifizierung in Neptune im Neptune-Benutzerhandbuch](#).

[Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2)

Kategorie: Identifizieren > Inventar > Kennzeichnung

Schweregrad: Niedrig

Art der Ressource: AWS::RDS::DBCluster

AWS Config -Regel: [neptune-cluster-copy-tags-to-snapshot-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Neptune-DB-Cluster so konfiguriert ist, dass bei der Erstellung der Snapshots alle Tags in Snapshots kopiert werden. Die Steuerung schlägt fehl, wenn ein Neptune-DB-Cluster nicht so konfiguriert ist, dass er Tags in Snapshots kopiert.

Die Identifizierung und Inventarisierung Ihrer IT-Ressourcen ist ein entscheidender Aspekt der Unternehmensführung und Sicherheit. Sie sollten Snapshots auf die gleiche Weise kennzeichnen wie ihre übergeordneten Amazon RDS-Datenbankcluster. Durch das Kopieren von Tags wird sichergestellt, dass die Metadaten für die DB-Snapshots mit denen der übergeordneten Datenbankcluster übereinstimmen und dass die Zugriffsrichtlinien für den DB-Snapshot auch mit denen der übergeordneten DB-Instance übereinstimmen.

Abhilfe

Informationen zum Kopieren von Tags in Snapshots für Neptune-DB-Cluster finden Sie unter [Kopieren von Tags in Neptune im Neptune-Benutzerhandbuch](#).

[Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: AWS::RDS::DBCluster

AWS Config -Regel: [neptune-cluster-multi-az-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob ein Amazon Neptune Neptune-DB-Cluster über Read-Replica-Instances in mehreren Availability Zones () verfügt. AZs Die Steuerung schlägt fehl, wenn der Cluster nur in einer AZ bereitgestellt wird.

Wenn eine AZ nicht verfügbar ist und während regelmäßiger Wartungsereignisse, dienen Read-Replicas als Failover-Ziele für die primäre Instanz. Wenn die primäre Instance ausfällt, stuft Neptune eine Read-Replica-Instance zur primären Instance herauf. Wenn Ihr DB-Cluster keine Read-Replica-Instances enthält, ist Ihr DB-Cluster bei einem Ausfall der primären Instance solange nicht verfügbar, bis sie neu erstellt wurde. Die Neuerstellung der primären Instance dauert erheblich länger als die Heraufstufung einer Read-Replica-Instance. Um eine hohe Verfügbarkeit zu gewährleisten,

empfehlen wir, eine oder mehrere Read-Replica-Instances zu erstellen, die dieselbe DB-Instance-Klasse wie die primäre Instance haben und sich in einer anderen als der primären Instance befinden. AZs

Abhilfe

Informationen zur Bereitstellung eines Neptune-DB-Clusters in mehreren AZs finden Sie unter [Read-Replica-DB-Instances in einem Neptune-DB-Cluster im Neptune-Benutzerhandbuch](#).

Security Hub Hub-Kontrollen für AWS Network Firewall

Diese AWS Security Hub Kontrollen bewerten den AWS Network Firewall Service und die Ressourcen. Die Steuerungen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[NetworkFirewall.1] Network firewalls sollten über mehrere Availability Zones hinweg bereitgestellt werden

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: AWS::NetworkFirewall::Firewall

AWS Config -Regel: [netfw-multi-az-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement bewertet, ob eine über mehrere Availability Zones verwaltete Firewall in mehreren Availability Zones (AZs) bereitgestellt AWS Network Firewall wird. Die Steuerung schlägt fehl, wenn eine Firewall nur in einer AZ bereitgestellt wird.

AWS Die globale Infrastruktur umfasst mehrere AWS-Regionen. AZs sind physisch getrennte, isolierte Standorte innerhalb jeder Region, die über hoch redundante Netzwerke mit geringer Latenz und hohen Durchsätzen verbunden sind. Durch die Bereitstellung einer Netzwerk-Firewall-Firewall

auf mehreren AZs Ebenen können Sie den Datenverkehr verteilen und zwischen diesen verlagern AZs, was Ihnen bei der Entwicklung hochverfügbarer Lösungen hilft.

Abhilfe

Bereitstellung einer Netzwerk-Firewall-Firewall über mehrere AZs

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im Navigationsbereich unter Network Firewall die Option Firewalls aus.
3. Wählen Sie auf der Seite Firewalls die Firewall aus, die Sie bearbeiten möchten.
4. Wählen Sie auf der Seite zu den Firewall-Details die Registerkarte Firewall-Details aus.
5. Wählen Sie im Abschnitt Verknüpfte Richtlinie und VPC die Option Bearbeiten aus.
6. Um eine neue AZ hinzuzufügen, wählen Sie Neues Subnetz hinzufügen. Wählen Sie die AZ und das Subnetz aus, die Sie verwenden möchten. Stellen Sie sicher, dass Sie mindestens zwei auswählen AZs.
7. Wählen Sie Speichern.

[NetworkFirewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (12), (4), NIST.800-53.r5 AC-2 (26), (9), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 NIST.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-9(7), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-4, NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8), NIST.800-171.R2 3.1.20, NIST.800-171.20, NIST.800-171.20 R2 3,13,1

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS::NetworkFirewall::LoggingConfiguration

AWS Config -Regel: [netfw-logging-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob die Protokollierung für eine AWS Network Firewall Firewall aktiviert ist. Die Steuerung schlägt fehl, wenn die Protokollierung für mindestens einen Protokolltyp nicht aktiviert ist oder wenn das Protokollierungsziel nicht existiert.

Mit der Protokollierung können Sie die Zuverlässigkeit, Verfügbarkeit und Performance Ihrer Firewalls aufrechterhalten. In Network Firewall erhalten Sie detaillierte Informationen zum Netzwerkverkehr, einschließlich der Zeit, zu der die Stateful-Engine einen Paketfluss empfangen hat, detaillierte Informationen zum Paketfluss und alle Stateful-Regelaktionen, die gegen den Paketfluss ausgeführt werden.

Abhilfe

Informationen zum Aktivieren der Protokollierung für eine Firewall finden Sie unter [Aktualisieren der Protokollierungskonfiguration einer Firewall](#) im AWS Network Firewall Entwicklerhandbuch.

[NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet haben

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.13.1

Kategorie: Schützen > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: AWS::NetworkFirewall::FirewallPolicy

AWS Config -Regel: [netfw-policy-rule-group-associated](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob einer Netzwerk-Firewall-Richtlinie statusbehaftete oder statuslose Regelgruppen zugeordnet sind. Die Steuerung schlägt fehl, wenn keine statusfreien oder statusbehafteten Regelgruppen zugewiesen werden.

Eine Firewall-Richtlinie legt fest, wie Ihre Firewall den Datenverkehr in Amazon Virtual Private Cloud (Amazon VPC) überwacht und verarbeitet. Die Konfiguration statusfreier und statusbehafteter Regelgruppen hilft beim Filtern von Paketen und Datenverkehrsströmen und definiert den standardmäßigen Umgang mit Datenverkehr.

Abhilfe

Informationen zum Hinzufügen einer Regelgruppe zu einer Netzwerk-Firewall-Richtlinie finden Sie unter [Aktualisieren einer Firewall-Richtlinie](#) im AWS Network Firewall Entwicklerhandbuch. Informationen zum Erstellen und Verwalten von Regelgruppen finden Sie unter [Regelgruppen in AWS Network Firewall](#).

[NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ sein.

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Schützen > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: AWS::NetworkFirewall::FirewallPolicy

AWS Config -Regel: [netfw-policy-default-action-full-packets](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `statelessDefaultActions: aws:drop,aws:forward_to_sfe`(nicht anpassbar)

Mit diesem Steuerelement wird geprüft, ob die statusfreie Standardaktion für vollständige Pakete für eine Richtlinie der Network Firewall die Option Verwerfen oder Weiterleiten ist. Die Steuerung ist erfolgreich, wenn Drop oder ausgewählt Forward ist, und schlägt fehl, wenn sie ausgewählt Pass ist.

Eine Firewall-Richtlinie legt fest, wie Ihre Firewall den Datenverkehr in Amazon VPC überwacht und verarbeitet. Sie konfigurieren statusfreie und statusbehaftete Regelgruppen, um Pakete und Datenverkehrsströme zu filtern. Wenn Sie standardmäßig die Einstellung verwenden, Pass kann dies zu unbeabsichtigtem Datenverkehr führen.

Abhilfe

Informationen zum Ändern Ihrer Firewall-Richtlinie finden Sie unter [Aktualisieren einer Firewall-Richtlinie im AWS Network Firewall Entwicklerhandbuch](#). Wählen Sie für Standardaktionen

ohne Status die Option Bearbeiten aus. Wählen Sie dann „Löschen“ oder „An statusbehaftete Regelgruppen weiterleiten“ als Aktion aus.

[NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ sein.

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-171.R2 3.1.3, NIST.800-171.r2 3.1.14, NIST.800-171.r2 3.13.1, NIST.800-171.r2 3.13.6

Kategorie: Schützen > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::NetworkFirewall::FirewallPolicy`

AWS Config -Regel: [netfw-policy-default-action-fragment-packets](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `statelessFragDefaultActions (Required)` : `aws:drop`, `aws:forward_to_sfe`(nicht anpassbar)

Dieses Steuerelement prüft, ob die standardmäßige statuslose Aktion für fragmentierte Pakete für eine Netzwerk-Firewall-Richtlinie Drop oder Forward ist. Die Steuerung ist erfolgreich, wenn Drop oder ausgewählt Forward ist, und schlägt fehl, wenn sie ausgewählt Pass ist.

Eine Firewall-Richtlinie legt fest, wie Ihre Firewall den Datenverkehr in Amazon VPC überwacht und verarbeitet. Sie konfigurieren statusfreie und statusbehaftete Regelgruppen, um Pakete und Datenverkehrsströme zu filtern. Wenn Sie standardmäßig die Einstellung verwenden, Pass kann dies zu unbeabsichtigtem Datenverkehr führen.

Abhilfe

Informationen zum Ändern Ihrer Firewall-Richtlinie finden Sie unter [Aktualisieren einer Firewall-Richtlinie im AWS Network Firewall Entwicklerhandbuch](#). Wählen Sie für Standardaktionen ohne Status die Option Bearbeiten aus. Wählen Sie dann „Löschen“ oder „An statusbehaftete Regelgruppen weiterleiten“ als Aktion aus.

[NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (21), (11), (16) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (5), NIST.800-53.r5 SC-7 NIST.800-171.r2 3.1.3, NIST.800-53.r5 SC-7 NIST.800-171.r2 3.1.14, NIST.800-171.r2 3.13.1, NIST.800-171.r2 3.13.6

Kategorie: Schützen > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: AWS::NetworkFirewall::RuleGroup

AWS Config -Regel: [netfw-stateless-rule-group-not-empty](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine statuslose Regelgruppe Regeln AWS Network Firewall enthält. Die Kontrolle schlägt fehl, wenn die Regelgruppe keine Regeln enthält.

Eine Regelgruppe enthält Regeln, die den Umgang Ihrer Firewall mit Datenverkehr in Ihrer VPC festlegen. Wenn eine leere statuslose Regelgruppe in einer Firewall-Richtlinie vorhanden ist, kann dies den Eindruck erwecken, dass die Regelgruppe den Datenverkehr verarbeitet. Wenn die statuslose Regelgruppe jedoch leer ist, verarbeitet sie keinen Datenverkehr.

Abhilfe

Informationen zum Hinzufügen von Regeln zu Ihrer Netzwerk-Firewall-Regelgruppe finden Sie unter [Aktualisieren einer statusbehafteten Regelgruppe](#) im AWS Network Firewall Entwicklerhandbuch. Wählen Sie auf der Seite mit den Firewall-Details für Stateless Rule Group die Option Bearbeiten aus, um Regeln hinzuzufügen.

[NetworkFirewall.7] Netzwerk-Firewall-Firewalls sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::NetworkFirewall::Firewall

AWS Config Regel: tagged-networkfirewall-firewall (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige Werte	Security Hub — Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob eine AWS Network Firewall Firewall über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn die Firewall keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Firewall mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` beginnen, werden ignoriert.

Ein Tag ist eine Markierung, die Sie einer AWS -Ressource zuordnen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Tags können Ihnen helfen, -Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tags verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC — Attribute-based access control) als Autorisierungsstrategie implementieren, die Berechtigungen auf der Grundlage von Tags definiert. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an AWS -Ressourcen anfügen. Sie können eine einzelne ABAC-Richtlinie oder einen separaten Richtlinienatz für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen zugelassen werden, wenn das Tag des

Prinzipals mit dem Tag der Ressource übereinstimmt. Weitere Informationen finden Sie unter [Was ist ABAC für AWS?](#) im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, einschließlich AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Netzwerk-Firewall-Firewall finden Sie unter [Tagging AWS Network Firewall resources](#) im AWS Network Firewall Developer Guide.

[NetworkFirewall.8] Firewall-Richtlinien für Netzwerk-Firewalls sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::NetworkFirewall::FirewallPolicy

AWS Config Regel: tagged-networkfirewall-firewallpolicy (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige Werte	Security Hub — Standardwert
requiredTagKeys	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß-	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Parameter	Beschreibung	Typ	Zulässige Werte	Security Hub — Standardwert

und Kleinschreibung unterschieden.

Dieses Steuerelement prüft, ob eine AWS Network Firewall Firewall-Richtlinie Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn die Firewall-Richtlinie keine Tagschlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Firewall-Richtlinie mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` beginnen, werden ignoriert.

Ein Tag ist eine Markierung, die Sie einer AWS -Ressource zuordnen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Tags können Ihnen helfen, -Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tags verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC — Attribute-based access control) als Autorisierungsstrategie implementieren, die Berechtigungen auf der Grundlage von Tags definiert. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an AWS -Ressourcen anfügen. Sie können eine einzelne ABAC-Richtlinie oder einen separaten Richtlinienatz für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen zugelassen werden, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt. Weitere Informationen finden Sie unter [Was ist ABAC für AWS?](#) im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche Informationen in Tags hinzu. Tags sind für viele zugängliche AWS-Services, einschließlich AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Netzwerk-Firewall-Richtlinie finden Sie unter [Tagging AWS Network Firewall resources](#) im AWS Network Firewall Developer Guide.

[NetworkFirewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Kategorie: Schützen > Netzwerksicherheit

Schweregrad: Mittel

Art der Ressource: `AWS::NetworkFirewall::Firewall`

AWS Config -Regel: [netfw-deletion-protection-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für eine AWS Network Firewall Firewall der Löschschutz aktiviert ist. Die Steuerung schlägt fehl, wenn der Löschschutz für eine Firewall nicht aktiviert ist.

AWS Network Firewall ist ein zustandsorientierter, verwalteter Dienst zur Netzwerk-Firewall und Erkennung von Eindringlingen, mit dem Sie den Datenverkehr zu, von oder zwischen Ihren Virtual Private Clouds () VPCs überprüfen und filtern können. Die Löschschutzeinstellung schützt vor versehentlichem Löschen der Firewall.

Abhilfe

Informationen zum Aktivieren des Löschschatzes für eine bestehende Netzwerk-Firewall-Firewall finden Sie unter [Aktualisieren einer Firewall](#) im AWS Network Firewall Entwicklerhandbuch. Wählen Sie unter Änderungsschutz die Option Aktivieren aus. Sie können den Löschschutz auch aktivieren, indem Sie die [UpdateFirewallDeleteProtection](#)API aufrufen und das DeleteProtection Feld auf setzen. `true`

[NetworkFirewall.10] Bei Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Kategorie: Schützen > Netzwerksicherheit

Schweregrad: Mittel

Art der Ressource: AWS::NetworkFirewall::Firewall

AWS Config -Regel: [netfw-subnet-change-protection-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der Subnetz-Änderungsschutz für eine AWS Network Firewall Firewall aktiviert ist. Die Steuerung schlägt fehl, wenn der Subnetzänderungsschutz für die Firewall nicht aktiviert ist.

AWS Network Firewall ist ein zustandsorientierter, verwalteter Dienst zur Netzwerk-Firewall und zur Erkennung von Eindringlingen, mit dem Sie den Datenverkehr zu, von oder zwischen Ihren Virtual Private Clouds (VPCs) untersuchen und filtern können. Wenn Sie den Subnetzänderungsschutz für eine Netzwerkfirewall-Firewall aktivieren, können Sie die Firewall vor versehentlichen Änderungen an den Subnetzzuordnungen der Firewall schützen.

Abhilfe

Informationen zur Aktivierung des Subnetzänderungsschutzes für eine bestehende Netzwerkfirewall-Firewall finden Sie unter [Aktualisieren einer Firewall](#) im AWS Network Firewall Entwicklerhandbuch.

Security Hub-Steuerelemente für Amazon OpenSearch Service

Diese AWS Security Hub Kontrollen bewerten den OpenSearch Service und die Ressourcen von Amazon OpenSearch Service (Service). Die Kontrollen sind möglicherweise nicht in allen verfügbaren AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

Bei [Opensearch.1] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein

Verwandte Anforderungen: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/7.2.1, (1), 3, 8, 8 (1), NIST.800-53.r5 SI-7 (6) NIST.800-53.r5 CA-9 NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-2

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: AWS::OpenSearch::Domain

AWS Config -Regel: [opensearch-encrypted-at-rest](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für OpenSearch Domänen die encryption-at-rest Konfiguration aktiviert ist. Die Prüfung schlägt fehl, wenn die Verschlüsselung im Ruhezustand nicht aktiviert ist.

Für eine zusätzliche Sicherheitsebene für vertrauliche Daten sollten Sie Ihre OpenSearch Service-Domain so konfigurieren, dass sie im Ruhezustand verschlüsselt wird. Wenn Sie die Verschlüsselung von Daten im Ruhezustand konfigurieren, AWS KMS werden Ihre Verschlüsselungsschlüssel gespeichert und verwaltet. Für die Verschlüsselung wird der Advanced Encryption Standard-Algorithmus mit 256-Bit-Schlüsseln (AES-256) AWS KMS verwendet.

Weitere Informationen zur OpenSearch Service-Verschlüsselung im Ruhezustand finden Sie unter [Verschlüsselung ruhender Daten für Amazon OpenSearch Service](#) im Amazon OpenSearch Service Developer Guide.

Abhilfe

Informationen zur Aktivierung der Verschlüsselung im Ruhezustand für neue und bestehende OpenSearch Domains finden Sie unter [Enabling encryption of data at rest](#) im Amazon OpenSearch Service Developer Guide.

[Opensearch.2] OpenSearch -Domains sollten nicht öffentlich zugänglich sein

Verwandte Anforderungen: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7), (21),

(11) NIST.800-53.r5 AC-3, (16) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (20), (21) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (3), (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen in VPC

Schweregrad: Kritisch

Art der Ressource: AWS::OpenSearch::Domain

AWS Config -Regel: [opensearch-in-vpc-only](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob sich OpenSearch Domänen in einer VPC befinden. Es bewertet nicht die Konfiguration des VPC-Subnetz-Routings, um den öffentlichen Zugriff zu bestimmen.

Sie sollten sicherstellen, dass OpenSearch Domänen nicht an öffentliche Subnetze angehängt sind. Informationen zu [ressourcenbasierten Richtlinien](#) finden Sie im Amazon OpenSearch Service Developer Guide. Sie sollten auch sicherstellen, dass Ihre VPC gemäß den empfohlenen bewährten Methoden konfiguriert ist. [Bewährte Sicherheitsmethoden für Ihre VPC](#) finden Sie im Amazon VPC-Benutzerhandbuch.

OpenSearch Domänen, die in einer VPC bereitgestellt werden, können über das private AWS Netzwerk mit VPC-Ressourcen kommunizieren, ohne das öffentliche Internet durchqueren zu müssen. Diese Konfiguration erhöht das Sicherheitsniveau, indem der Zugriff auf die Daten während der Übertragung eingeschränkt wird. VPCs bieten eine Reihe von Netzwerkkontrollen, um den Zugriff auf OpenSearch Domänen zu sichern, einschließlich Netzwerk-ACL und Sicherheitsgruppen. Security Hub empfiehlt, öffentliche OpenSearch Domains zu migrieren, VPCs um diese Kontrollen nutzen zu können.

Abhilfe

Wenn Sie eine Domäne mit einem öffentlichen Endpunkt erstellen, können Sie sie später nicht in einer VPC platzieren. Sie müssen stattdessen eine neue Domäne erstellen und die Daten übernehmen. Umgekehrt gilt dies auch. Wenn Sie eine Domäne innerhalb einer VPC erstellen, kann sie keinen öffentlichen Endpunkt haben. Stattdessen müssen Sie entweder [eine andere Domäne erstellen](#) oder dieses Steuerelement deaktivieren.

Anweisungen finden Sie unter [Starten Ihrer Amazon OpenSearch Service-Domains innerhalb einer VPC](#) im Amazon OpenSearch Service Developer Guide.

[Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden

Verwandte Anforderungen: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 3, 3 (NIST.800-53.r5 SC-23), NIST.800-53.r5 SC-7 (4),, NIST.800-53.r5 SC-8 (1) NIST.800-53.r5 SC-8, (2) NIST.800-53.r5 SC-8

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: AWS::OpenSearch::Domain

AWS Config -Regel: [opensearch-node-to-node-encryption-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für OpenSearch Domänen die node-to-node Verschlüsselung aktiviert ist. Diese Kontrolle schlägt fehl, wenn die node-to-node Verschlüsselung in der Domain deaktiviert ist.

HTTPS (TLS) kann verwendet werden, um zu verhindern, dass potenzielle Angreifer den Netzwerkverkehr mit person-in-the-middle oder ähnlichen Angriffen abhören oder manipulieren. Nur verschlüsselte Verbindungen über HTTPS (TLS) sollten zugelassen werden. Durch die Aktivierung der node-to-node Verschlüsselung für OpenSearch Domänen wird sichergestellt, dass die Kommunikation innerhalb des Clusters während der Übertragung verschlüsselt wird.

Mit dieser Konfiguration kann es zu Leistungseinbußen kommen. Sie sollten sich der Leistungseinbußen bewusst sein und diese testen, bevor Sie diese Option aktivieren.

Abhilfe

Informationen zum Aktivieren der node-to-node Verschlüsselung für eine OpenSearch Domain finden Sie unter [node-to-nodeEnabling encryption](#) im Amazon OpenSearch Service Developer Guide.

Die Protokollierung von [Opensearch.4] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 (9), NIST.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS::OpenSearch::Domain

AWS Config -Regel: [opensearch-logs-to-cloudwatch](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- logtype = 'error'(nicht anpassbar)

Dieses Steuerelement prüft, ob OpenSearch Domänen so konfiguriert sind, dass sie CloudWatch Fehlerprotokolle an Logs senden. Dieses Steuerelement schlägt fehl, wenn die Fehlerprotokollierung für eine Domäne nicht aktiviert CloudWatch ist.

Sie sollten Fehlerprotokolle für OpenSearch Domänen aktivieren und diese CloudWatch Protokolle zur Aufbewahrung und Bearbeitung an Logs senden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Abhilfe

Informationen zum Aktivieren der Protokollveröffentlichung finden Sie unter [Aktivieren der Protokollveröffentlichung \(Konsole\)](#) im Amazon OpenSearch Service Developer Guide.

Für [Opensearch.5] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 (9), NIST.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5

AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8), PCI DSS v4.0.1/10.2.1

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS::OpenSearch::Domain

AWS Config -Regel: [opensearch-audit-logging-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `cloudWatchLogsLogGroupArnList`(nicht anpassbar) — Security Hub füllt diesen Parameter nicht aus. Durch Kommas getrennte Liste von CloudWatch Logs-Log-Gruppen, die für Audit-Logs konfiguriert werden sollten.

Dieses Steuerelement prüft, ob in OpenSearch Domänen die Auditprotokollierung aktiviert ist. Dieses Steuerelement schlägt fehl, wenn für eine OpenSearch Domäne die Überwachungsprotokollierung nicht aktiviert ist.

Auditprotokolle sind in hohem Maße anpassbar. Sie ermöglichen es Ihnen, Benutzeraktivitäten auf Ihren OpenSearch Clustern nachzuverfolgen, einschließlich erfolgreicher und fehlgeschlagener Authentifizierungen, Anfragen an, Indexänderungen und eingehende Suchanfragen.

Abhilfe

Anweisungen zur Aktivierung von Audit-Logs finden Sie unter [Aktivieren von Audit-Logs](#) im Amazon OpenSearch Service Developer Guide.

[Opensearch.6] OpenSearch Domains sollten mindestens drei Datenknoten haben

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: AWS::OpenSearch::Domain

AWS Config -Regel: [opensearch-data-node-fault-tolerance](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob OpenSearch Domänen mit mindestens drei Datenknoten konfiguriert sind und `zoneAwarenessEnabled` ist `true`. Dieses Steuerelement schlägt für eine OpenSearch Domäne fehl, wenn sie `instanceCount` weniger als 3 `zoneAwarenessEnabled` ist oder ist `false`.

Um eine hohe Verfügbarkeit und Fehlertoleranz auf Clusterebene zu erreichen, sollte eine OpenSearch Domäne über mindestens drei Datenknoten verfügen. Durch die Bereitstellung einer OpenSearch Domäne mit mindestens drei Datenknoten wird der Clusterbetrieb gewährleistet, falls ein Knoten ausfällt.

Abhilfe

Um die Anzahl der Datenknoten in einer OpenSearch Domäne zu ändern

1. Melden Sie sich bei der AWS Konsole an und öffnen Sie die Amazon OpenSearch Service-Konsole unter <https://console.aws.amazon.com/aos/>.
2. Wählen Sie unter Meine Domains den Namen der Domain aus, die Sie bearbeiten möchten, und wählen Sie Bearbeiten aus.
3. Stellen Sie unter Datenknoten die Anzahl der Knoten auf eine Zahl größer als ein. Wenn Sie in drei Availability Zones bereitstellen, legen Sie die Zahl auf ein Vielfaches von drei fest, um eine gleichmäßige Verteilung auf die Availability Zones sicherzustellen.
4. Wählen Sie Absenden aus.

Für [Opensearch.7] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1), (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6

Kategorie: Schützen > Secure Access Management > Eingeschränkte sensible API-Aktionen

Schweregrad: Hoch

Art der Ressource: AWS::OpenSearch::Domain

AWS Config -Regel: [opensearch-access-control-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für OpenSearch Domänen eine differenzierte Zugriffskontrolle aktiviert ist. Die Steuerung schlägt fehl, wenn die feinkörnige Zugriffskontrolle nicht aktiviert ist. Für die differenzierte Zugriffskontrolle muss `advanced-security-options` der OpenSearch Parameter `update-domain-config` aktiviert sein.

Eine detaillierte Zugriffskontrolle bietet zusätzliche Möglichkeiten, den Zugriff auf Ihre Daten bei Amazon OpenSearch Service zu kontrollieren.

Abhilfe

Informationen zur Aktivierung der feinkörnigen Zugriffskontrolle finden Sie unter [Feinkörnige Zugriffskontrolle in Amazon OpenSearch Service im Amazon OpenSearch Service Developer Guide](#).

[Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 AC-1 7 (2), (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 NIST.800-53.r5 IA-5 (3), 3, 3, NIST.800-53.r5 SC-1 3 (3), NIST.800-53.r5 SC-2 (4), (1), NIST.800-53.r5 SC-7 (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.R5 SI-7 NIST.800-53.r5 SC-8 (6) NIST.800-53.r5 SC-2

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: AWS::OpenSearch::Domain

AWS Config -Regel: [opensearch-https-required](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `tlsPolicies`: Policy-Min-TLS-1-2-PFS-2023-10(nicht anpassbar)

Diese Steuerung prüft, ob ein Amazon OpenSearch Service-Domain-Endpunkt so konfiguriert ist, dass er die neueste TLS-Sicherheitsrichtlinie verwendet. Die Kontrolle schlägt fehl, wenn der

OpenSearch Domain-Endpunkt nicht für die Verwendung der neuesten unterstützten Richtlinie konfiguriert ist oder wenn er HTTPs nicht aktiviert ist.

HTTPS (TLS) kann verwendet werden, um zu verhindern, dass potenzielle Angreifer person-in-the-middle oder ähnliche Angriffe verwenden, um den Netzwerkverkehr zu belauschen oder zu manipulieren. Nur verschlüsselte Verbindungen über HTTPS (TLS) sollten zugelassen werden. Die Verschlüsselung von Daten während der Übertragung kann die Leistung beeinträchtigen. Sie sollten Ihre Anwendung mit dieser Funktion testen, um das Leistungsprofil und die Auswirkungen von TLS zu verstehen. TLS 1.2 bietet mehrere Sicherheitsverbesserungen gegenüber früheren Versionen von TLS.

Abhilfe

Verwenden Sie den [UpdateDomainConfig](#) API-Vorgang, um die TLS-Verschlüsselung zu aktivieren. Konfigurieren Sie das [DomainEndpointOptions](#) Feld, um den Wert für anzugeben `TLSecurityPolicy`. Weitere Informationen finden Sie unter [Node-to-node Verschlüsselung](#) im Amazon OpenSearch Service Developer Guide.

[Opensearch.9] OpenSearch -Domains sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::OpenSearch::Domain`

AWS Config Regel: `tagged-opensearch-domain` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS	No default value

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen.	

Dieses Steuerelement prüft, ob eine Amazon OpenSearch Service-Domain Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind `requiredTagKeys`. Die Kontrolle schlägt fehl, wenn die Domain keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Domain mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `aws:` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der [Allgemeine AWS-Referenz](#).

Abhilfe

Informationen zum Hinzufügen von Tags zu einer OpenSearch Service-Domain finden Sie unter [Arbeiten mit Tags](#) im Amazon OpenSearch Service Developer Guide.

Auf [Opensearch.10] OpenSearch -Domains sollte das neueste Softwareupdate installiert sein

Verwandte Anforderungen: NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), NIST.800-53.R5 SI-2 (5), PCI DSS v4.0.1/6.3.3

Kategorie: Identifizieren > Sicherheitslücken-, Patch- und Versionsverwaltung

Schweregrad: Niedrig

Art der Ressource: AWS::OpenSearch::Domain

AWS Config -Regel: [opensearch-update-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob auf einer Amazon OpenSearch Service-Domain das neueste Softwareupdate installiert ist. Die Kontrolle schlägt fehl, wenn ein Softwareupdate verfügbar, aber nicht für die Domain installiert ist.

OpenSearch Service-Softwareupdates bieten die neuesten Plattformkorrekturen, Updates und Funktionen, die für die Umgebung verfügbar sind. Die up-to-date Beibehaltung der Patch-Installation trägt dazu bei, die Sicherheit und Verfügbarkeit der Domain aufrechtzuerhalten. Wenn bei den erforderlichen Updates keine Maßnahmen ergriffen werden, wird die Service-Software automatisch aktualisiert (in der Regel nach 2 Wochen). Wir empfehlen, Updates in Zeiten mit geringem Datenverkehr auf der Domain zu planen, um Dienstunterbrechungen zu minimieren.

Abhilfe

Informationen zur Installation von Softwareupdates für eine OpenSearch Domain finden Sie unter [Ein Update starten](#) im Amazon OpenSearch Service Developer Guide.

[Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2, NIST.800-53.r5 SC-5, NIST.800-53.r5 SC-3 6, NIST.800-53.R5 SI-13

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Niedrig

Art der Ressource: AWS::OpenSearch::Domain

AWS Config -Regel: [opensearch-primary-node-fault-tolerance](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob eine Amazon OpenSearch Service-Domain mit mindestens drei dedizierten Primärknoten konfiguriert ist. Die Kontrolle schlägt fehl, wenn die Domain weniger als drei dedizierte Primärknoten hat.

OpenSearch Der Dienst verwendet dedizierte Primärknoten, um die Clusterstabilität zu erhöhen. Ein dedizierter primärer Knoten führt Clusterverwaltungsaufgaben aus, speichert jedoch keine Daten und reagiert auch nicht auf Anfragen zum Hochladen von Daten. Wir empfehlen die Verwendung von Multi-AZ mit Standby, wodurch jeder OpenSearch Produktionsdomäne drei dedizierte Primärknoten hinzugefügt werden.

Abhilfe

Informationen zum Ändern der Anzahl der Primärknoten für eine OpenSearch Domain finden Sie unter [Erstellen und Verwalten von Amazon OpenSearch Service-Domains](#) im Amazon OpenSearch Service Developer Guide.

Security Hub-Steuerungen für AWS Private CA

Diese AWS Security Hub Kontrollen bewerten den AWS Private Certificate Authority (AWS Private CA) Dienst und die Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[PCA.1] AWS Private CA Root-Zertifizierungsstelle sollte deaktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Niedrig

Art der Ressource: AWS::ACMPCA::CertificateAuthority

AWS Config -Regel: [acm-pca-root-ca-disabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob es AWS Private CA eine deaktivierte Stammzertifizierungsstelle (CA) gibt. Die Steuerung schlägt fehl, wenn die Stammzertifizierungsstelle aktiviert ist.

Mit AWS Private CA können Sie eine Zertifizierungsstellenhierarchie erstellen, die eine Stammzertifizierungsstelle und eine untergeordnete CAs Zertifizierungsstelle umfasst. Sie sollten die Verwendung der Stammzertifizierungsstelle für tägliche Aufgaben minimieren, insbesondere in Produktionsumgebungen. Die Stammzertifizierungsstelle sollte nur zur Ausstellung von Zertifikaten für Zwischenzertifikate verwendet werden CAs. Auf diese Weise kann die Stammzertifizierungsstelle vor Gefahren geschützt aufbewahrt werden, während die CAs Zwischenzertifizierungsstelle die tägliche Aufgabe der Ausstellung von Endzertifikaten übernimmt.

Abhilfe

Informationen zum Deaktivieren der Stammzertifizierungsstelle finden Sie unter [CA-Status aktualisieren](#) im AWS Private Certificate Authority Benutzerhandbuch.

[PCA.2] AWS Private CA-Zertifizierungsstellen sollten gekennzeichnet werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::ACMPCA::CertificateAuthority

AWS Config -Regel: acmpca-certificate-authority-tagged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS private Zertifizierungsstelle über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredKeyTags` definiert sind. Die Kontrolle schlägt fehl, wenn die Zertifizierungsstelle keine Tagschlüssel hat oder wenn sie nicht über alle im Parameter angegebenen Schlüssel verfügt `requiredKeyTags`. Wenn der Parameter `requiredKeyTags` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Zertifizierungsstelle mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` , werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen in Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Tagging finden Sie unter [Bewährte Methoden und Strategien](#) im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Abhilfe

Informationen zum Hinzufügen von Stichwörtern zu einer AWS privaten Zertifizierungsstelle finden Sie unter [Hinzufügen von Stichwörtern für Ihre private Zertifizierungsstelle](#) im AWS Private Certificate Authority Benutzerhandbuch.

Security Hub-Steuerelemente für Amazon RDS

Diese AWS Security Hub Kontrollen bewerten den Service und die Ressourcen des Amazon Relational Database Service (Amazon RDS). Die Steuerelemente sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[RDS.1] Der RDS-Snapshot sollte privat sein

Verwandte Anforderungen: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, PCI DSS v3.2.1/7.2.1, NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7), (21), (11) NIST.800-53.r5 AC-3, (16), (20) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-6, (3) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Kritisch

Ressourcentyp: AWS::RDS::DBClusterSnapshot, AWS::RDS::DBSnapshot

AWS Config -Regel: [rds-snapshots-public-prohibited](#)

Zeitplantyp: Änderung ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Amazon RDS-Snapshots öffentlich sind. Die Steuerung schlägt fehl, wenn RDS-Snapshots öffentlich sind. Dieses Steuerelement bewertet RDS-Instances, Aurora-DB-Instances, Neptune-DB-Instances und Amazon DocumentDB-Cluster.

RDS-Snapshots werden verwendet, um die Daten auf Ihren RDS-Instances zu einem bestimmten Zeitpunkt zu sichern. Sie können verwendet werden, um frühere Zustände von RDS-Instances wiederherzustellen.

Ein RDS-Snapshot darf nur öffentlich sein, wenn dies beabsichtigt ist. Wenn Sie einen unverschlüsselten manuellen Snapshot als öffentlich freigeben, wird der Snapshot dadurch für alle verfügbar. AWS-Konten Dies kann zu einer unbeabsichtigten Offenlegung von Daten Ihrer RDS-Instance führen.

Beachten Sie, dass die AWS Config Regel die Änderung möglicherweise bis zu 12 Stunden lang nicht erkennen kann, wenn die Konfiguration so geändert wird, dass sie öffentlich zugänglich ist. Bis die AWS Config Regel die Änderung erkennt, ist die Prüfung erfolgreich, obwohl die Konfiguration gegen die Regel verstößt.

Weitere Informationen zum Teilen eines DB-Snapshots finden Sie unter [Freigeben eines DB-Snapshots](#) im Amazon RDS-Benutzerhandbuch.

Abhilfe

Informationen zum Entfernen des öffentlichen Zugriffs auf RDS-Snapshots finden Sie unter [Einen Snapshot teilen](#) im Amazon RDS-Benutzerhandbuch. Für die Sichtbarkeit von DB-Snapshots wählen wir Privat.

[RDS.2] RDS-DB-Instances sollten, wie in der Konfiguration festgelegt, den öffentlichen Zugriff verbieten PubliclyAccessible

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/2.3.3., NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-4, (11), (16) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (5), NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6 1/7.2.1, PCI DSS v4.0.1/1.4.4 NIST.800-53.r5 SC-7

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Kritisch

Art der Ressource: AWS::RDS::DBInstance

AWS Config -Regel: [rds-instance-public-access-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Amazon RDS-Instances öffentlich zugänglich sind, indem es das PubliclyAccessible Feld im Instance-Konfigurationselement auswertet.

Neptune-DB-Instances und Amazon DocumentDB-Cluster haben das PubliclyAccessible Flag nicht und können nicht ausgewertet werden. Diese Kontrolle kann jedoch immer noch Ergebnisse für diese Ressourcen generieren. Sie können diese Ergebnisse unterdrücken.

Der PubliclyAccessible-Wert in der RDS-Instance-Konfiguration gibt an, ob die DB-Instance öffentlich zugänglich ist. Wenn die DB-Instance mit PubliclyAccessible konfiguriert ist, handelt es sich um eine mit dem Internet verbundene Instance mit einem öffentlich auflösbaren DNS-Namen, der in eine öffentliche IP-Adresse aufgelöst wird. Wenn die DB-Instance nicht öffentlich zugänglich ist, handelt es sich um eine interne Instance mit einem DNS-Namen, der in eine private IP-Adresse aufgelöst wird.

Sofern Sie nicht beabsichtigen, dass Ihre RDS-Instance öffentlich zugänglich ist, sollte die RDS-Instance nicht mit PubliclyAccessible Value konfiguriert werden. Dadurch könnte unnötiger Datenverkehr zu Ihrer Datenbank-Instance entstehen.

Abhilfe

Informationen zum Entfernen des öffentlichen Zugriffs auf RDS-DB-Instances finden Sie unter [Ändern einer Amazon RDS-DB-Instance](#) im Amazon RDS-Benutzerhandbuch. Wählen Sie für öffentlichen Zugriff die Option Nein.

[RDS.3] Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein.

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/2.3.1, CIS AWS Foundations Benchmark v1.4.0/2.3.1, (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 NIST.800-53.r5 CA-9 (1), (10), NIST.800-53.r5 NIST.800-53.r5 SC-2 SI-7 (6) NIST.800-53.r5 SC-7

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: AWS::RDS::DBInstance

AWS Config -Regel: [rds-storage-encrypted](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob die Speicherverschlüsselung für Ihre Amazon RDS-DB-Instances aktiviert ist.

Diese Steuerung ist für RDS-DB-Instances vorgesehen. Es kann jedoch auch Ergebnisse für Aurora-DB-Instances, Neptune-DB-Instances und Amazon DocumentDB-Cluster generieren. Wenn diese Ergebnisse nicht nützlich sind, können Sie sie unterdrücken.

Um eine zusätzliche Sicherheitsebene für Ihre sensiblen Daten in RDS-DB-Instances zu erhalten, sollten Sie Ihre RDS-DB-Instances so konfigurieren, dass sie im Ruhezustand verschlüsselt werden. Um Ihre RDS-DB-Instances und Snapshots im Ruhezustand zu verschlüsseln, aktivieren Sie die Verschlüsselungsoption für Ihre RDS-DB-Instances. Daten, die im Ruhezustand verschlüsselt werden, umfassen den zugehörigen Speicherplatz für DB-Instances, deren automatisierte Backups, Read Replicas und Snapshots.

RDS-verschlüsselte DB-Instances verwenden den offenen Standard AES-256-Verschlüsselungsalgorithmus, um Ihre Daten auf dem Server zu verschlüsseln, der Ihre RDS-DB-Instance hostet. Nachdem Ihre Daten verschlüsselt wurden, verarbeitet Amazon RDS die Authentifizierung des Zugriffs und die Entschlüsselung Ihrer Daten transparent und mit minimalen Auswirkungen auf die Leistung. Sie müssen Ihre Datenbank-Client-Anwendungen nicht ändern, um die Verschlüsselung anzuwenden.

Die Amazon RDS-Verschlüsselung ist derzeit für alle Datenbank-Engines und Speichertypen verfügbar. Amazon RDS-Verschlüsselung ist für die meisten DB-Instance-Klassen verfügbar. Informationen zu DB-Instance-Klassen, die die Amazon RDS-Verschlüsselung nicht unterstützen, finden Sie unter [Verschlüsseln von Amazon RDS-Ressourcen](#) im Amazon RDS-Benutzerhandbuch.

Abhilfe

Informationen zur Verschlüsselung von DB-Instances in Amazon RDS finden Sie unter [Verschlüsseln von Amazon RDS-Ressourcen](#) im Amazon RDS-Benutzerhandbuch.

[RDS.4] RDS-Cluster-Snapshots und Datenbank-Snapshots sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 (1), (10), NIST.800-53.R5 NIST.800-53.r5 SC-2 SI-7 NIST.800-53.r5 SC-7 (6)

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Ressourcentyp: AWS::RDS::DBClusterSnapshot, AWS::RDS::DBSnapshot

AWS Config -Regel: [rds-snapshot-encrypted](#)

Zeitplantyp: Änderung ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein RDS-DB-Snapshot verschlüsselt ist. Die Steuerung schlägt fehl, wenn ein RDS-DB-Snapshot nicht verschlüsselt ist.

Dieses Steuerelement ist für RDS-DB-Instances vorgesehen. Es kann jedoch auch Ergebnisse für Snapshots von Aurora-DB-Instances, Neptune-DB-Instances und Amazon DocumentDB-Clustern generieren. Wenn diese Ergebnisse nicht nützlich sind, können Sie sie unterdrücken.

Durch die Verschlüsselung von Daten im Ruhezustand wird das Risiko verringert, dass ein nicht authentifizierter Benutzer Zugriff auf Daten erhält, die auf der Festplatte gespeichert sind. Daten in RDS-Snapshots sollten im Ruhezustand verschlüsselt werden, um eine zusätzliche Sicherheitsebene zu gewährleisten.

Abhilfe

Informationen zum Verschlüsseln eines RDS-Snapshots finden Sie unter [Verschlüsseln von Amazon RDS-Ressourcen](#) im Amazon RDS-Benutzerhandbuch. Wenn Sie eine RDS-DB-Instance verschlüsseln, umfassen die verschlüsselten Daten den der Instance zugrunde liegenden Speicher, ihre automatisierten Backups, Read Replicas und Snapshots.

Sie können eine RDS-DB-Instance nur verschlüsseln, wenn Sie sie erstellen, nicht nachdem die DB-Instance erstellt wurde. Da es jedoch möglich ist, die Kopie eines unverschlüsselten Snapshots zu verschlüsseln, können Sie quasi eine Verschlüsselung zu einer unverschlüsselten DB-Instance

hinzufügen. Dies lässt sich durchführen, indem Sie einen Snapshot von Ihrer DB-Instance erstellen und dann eine verschlüsselte Kopie dieses Snapshots erstellen. Anschließend können Sie Ihre DB-Instance aus dem verschlüsselten Snapshot wiederherstellen und verfügen so über eine verschlüsselte Kopie Ihrer ursprünglichen DB-Instance.

[RDS.5] RDS-DB-Instances sollten mit mehreren Availability Zones konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: AWS::RDS::DBInstance

AWS Config -Regel: [rds-multi-az-support](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Hochverfügbarkeit für Ihre RDS-DB-Instances aktiviert ist. Die Steuerung schlägt fehl, wenn eine RDS-DB-Instance nicht mit mehreren Availability Zones (AZs) konfiguriert ist. Diese Steuerung gilt nicht für RDS-DB-Instances, die Teil einer Multi-AZ-DB-Cluster-Bereitstellung sind.

Die Konfiguration von Amazon RDS-DB-Instances mit AZs trägt dazu bei, die Verfügbarkeit der gespeicherten Daten sicherzustellen. Multi-AZ-Bereitstellungen ermöglichen einen automatisierten Failover bei Problemen mit der AZ-Verfügbarkeit und während der regulären RDS-Wartung.

Abhilfe

Um Ihre DB-Instances in mehreren bereitzustellen AZs, [ändern Sie eine DB-Instance zu einer Multi-AZ-DB-Instance-Bereitstellung](#) im Amazon RDS-Benutzerhandbuch.

[RDS.6] Die erweiterte Überwachung sollte für RDS-DB-Instances konfiguriert werden

Verwandte Anforderungen: NIST.800-53.R5 NIST.800-53.r5 CA-7 SI-2

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config -Regel: [rds-enhanced-monitoring-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert	
<code>monitoringInterval</code>	Anzahl der Sekunden zwischen den Intervallen zur Erfassung von Überwachungsmetriken	Enum	1, 5, 10, 15, 30, 60	Kein Standardwert	

Dieses Steuerelement prüft, ob die erweiterte Überwachung für eine Amazon Relational Database Service (Amazon RDS) -DB-Instance aktiviert ist. Die Steuerung schlägt fehl, wenn die erweiterte Überwachung für die Instance nicht aktiviert ist. Wenn Sie einen benutzerdefinierten Wert für den `monitoringInterval` Parameter angeben, ist die Steuerung nur erfolgreich, wenn die Metriken zur erweiterten Überwachung für die Instance im angegebenen Intervall erfasst werden.

In Amazon RDS ermöglicht Enhanced Monitoring eine schnellere Reaktion auf Leistungsänderungen in der zugrunde liegenden Infrastruktur. Diese Leistungsänderungen können zu einer mangelnden Verfügbarkeit der Daten führen. Enhanced Monitoring bietet Echtzeit-Metriken des Betriebssystems, auf dem Ihre RDS-DB-Instance läuft. Auf der Instance ist ein Agent installiert. Der Agent kann Metriken genauer abrufen, als dies auf der Hypervisor-Ebene möglich ist.

Metriken von Enhanced Monitoring sind nützlich, um zu sehen, wie unterschiedliche Prozesse oder Threads auf einer DB-Instance die CPU nutzen. Weitere Informationen finden Sie unter [Enhanced Monitoring](#) (Erweiterte Überwachung) im Amazon-RDS-Benutzerhandbuch.

Abhilfe

Detaillierte Anweisungen zur Aktivierung von Enhanced Monitoring für Ihre DB-Instance finden Sie unter [Enhanced Monitoring einrichten und aktivieren](#) im Amazon RDS-Benutzerhandbuch.

[RDS.7] Bei RDS-Clustern sollte der Löschschutz aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Kategorie: Schützen > Datenschutz > Schutz vor Datenlöschung

Schweregrad: Niedrig

Art der Ressource: AWS::RDS::DBCluster

AWS Config -Regel: [rds-cluster-deletion-protection-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für einen RDS-DB-Cluster der Löschschutz aktiviert ist. Die Steuerung schlägt fehl, wenn für einen RDS-DB-Cluster kein Löschschutz aktiviert ist.

Dieses Steuerelement ist für RDS-DB-Instances vorgesehen. Es kann jedoch auch Ergebnisse für Aurora-DB-Instances, Neptune-DB-Instances und Amazon DocumentDB-Cluster generieren. Wenn diese Ergebnisse nicht nützlich sind, können Sie sie unterdrücken.

Die Aktivierung des Cluster-Löschschutzes bietet zusätzlichen Schutz vor versehentlichem Löschen von Datenbanken oder vor dem Löschen durch eine nicht autorisierte Entität.

Wenn der Löschschutz aktiviert ist, kann ein RDS-Cluster nicht gelöscht werden. Bevor eine Löschanforderung erfolgreich sein kann, muss der Löschschutz deaktiviert werden.

Abhilfe

Informationen zum Aktivieren des Löschschutzes für einen RDS-DB-Cluster finden Sie unter [Ändern des DB-Clusters mithilfe der Konsole, der CLI und der API](#) im Amazon RDS-Benutzerhandbuch.

Wählen Sie für den Löschschutz die Option Löschschutz aktivieren.

[RDS.8] Für RDS-DB-Instances sollte der Löschschutz aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Schützen > Datenschutz > Schutz vor Datenlöschung

Schweregrad: Niedrig

Art der Ressource: AWS::RDS::DBInstance

AWS Config -Regel: [rds-instance-deletion-protection-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- databaseEngines: mariadb,mysql,custom-oracle-ee,oracle-ee-cdb,oracle-se2-cdb,oracle-ee,oracle-se2,oracle-se1,oracle-se,postgres,sqlserver-ee,sqlserver-se,sqlserver-ex,sqlserver-web (nicht anpassbar)

Dieses Steuerelement prüft, ob für Ihre RDS-DB-Instances, die eine der aufgelisteten Datenbank-Engines verwenden, der Löschschutz aktiviert ist. Die Steuerung schlägt fehl, wenn für eine RDS-DB-Instance kein Löschschutz aktiviert ist.

Die Aktivierung des Schutzes vor dem Löschen von Instances ist eine zusätzliche Schutzebene gegen das versehentliche Löschen von Datenbanken oder das Löschen durch eine nicht autorisierte Entität.

Solange der Löschschutz aktiviert ist, kann eine RDS-DB-Instance nicht gelöscht werden. Bevor eine Löschanforderung erfolgreich sein kann, muss der Löschschutz deaktiviert werden.

Abhilfe

Informationen zum Aktivieren des Löschschutzes für eine RDS-DB-Instance finden Sie unter [Ändern einer Amazon RDS-DB-Instance](#) im Amazon RDS-Benutzerhandbuch. Wählen Sie für den Löschschutz die Option Löschschutz aktivieren.

[RDS.9] RDS-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), (10), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 NIST.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8), PCI DSS v4.0.1/10.2.1

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Ressourcentyp: AWS::RDS::DBInstance

AWS Config -Regel: [rds-logging-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Amazon RDS-DB-Instance so konfiguriert ist, dass sie die folgenden Protokolle in Amazon CloudWatch Logs veröffentlicht. Die Kontrolle schlägt fehl, wenn die Instance nicht so konfiguriert ist, dass sie die folgenden CloudWatch Protokolle in Logs veröffentlicht:

- Oracle: Alert, Audit, Trace, Listener
- PostgreSQL: Postgresql, Aktualisierung
- MySQL: Audit, Fehler, Allgemein, SlowQuery
- MariaDB: Audit, Fehler, Allgemein, SlowQuery
- SQL Server: Fehler, Agent
- Aurora: Prüfung, Fehler, Allgemein, SlowQuery
- Aurora-MySQL: Prüfung, Fehler, Allgemein, SlowQuery
- Aurora-PostgreSQL: PostgreSQL

Für RDS-Datenbanken sollten die entsprechenden Protokolle aktiviert sein. Die Datenbankprotokollierung bietet detaillierte Aufzeichnungen der an RDS gestellten Anfragen. Datenbankprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Abhilfe

Informationen zum Veröffentlichen von RDS-Datenbankprotokollen in CloudWatch Logs finden Sie [unter Spezifizieren der in CloudWatch Logs zu veröffentlichenden Logs](#) im Amazon RDS-Benutzerhandbuch.

[RDS.10] Die IAM-Authentifizierung sollte für RDS-Instances konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15) NIST.800-53.r5 AC-3, (7), NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6

Kategorie: Schützen > Sichere Zugriffsverwaltung > Passwortlose Authentifizierung

Schweregrad: Mittel

Art der Ressource: AWS::RDS::DBInstance

AWS Config -Regel: [rds-instance-iam-authentication-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für eine RDS-DB-Instance die IAM-Datenbankauthentifizierung aktiviert ist. Die Steuerung schlägt fehl, wenn die IAM-Authentifizierung nicht für RDS-DB-Instances konfiguriert ist. Diese Steuerung bewertet nur RDS-Instances mit den folgenden Engine-Typen: mysql, postgres, aurora, aurora-mysql, aurora-postgresql, und mariadb. Eine RDS-Instanz muss sich außerdem in einem der folgenden Zustände befinden, damit ein Ergebnis generiert werden kann: available, backing-up, storage-optimization, oder storage-full.

Die IAM-Datenbankauthentifizierung ermöglicht die Authentifizierung von Datenbank-Instances mit einem Authentifizierungstoken anstelle eines Kennworts. Der Netzwerkverkehr zur und von der Datenbank wird mit SSL verschlüsselt. Weitere Informationen finden Sie unter [IAM-Datenbank-Authentifizierung](#) im Amazon Aurora-Benutzerhandbuch.

Abhilfe

Informationen zur Aktivierung der IAM-Datenbankauthentifizierung auf einer RDS-DB-Instance finden Sie unter [Aktivieren und Deaktivieren der IAM-Datenbankauthentifizierung](#) im Amazon RDS-Benutzerhandbuch.

[RDS.11] Bei RDS-Instances sollten automatische Backups aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-12, NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Backups aktiviert

Schweregrad: Mittel

Art der Ressource: AWS::RDS::DBInstance

AWS Config -Regel: [db-instance-backup-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Standardwert
backupRetentionMinimum	Minimale Aufbewahrungsdauer für Backups in Tagen	Ganzzahl	7 auf 35	7
checkReadReplicas	Überprüft, ob für RDS-DB-Instances Backups für Read Replicas aktiviert sind	Boolesch	Nicht anpassbar	false

Diese Kontrolle prüft, ob für eine Amazon Relational Database Service Service-Instance automatische Backups aktiviert sind und ob eine Aufbewahrungsfrist für Backups größer oder gleich dem angegebenen Zeitraum ist. Read Replicas sind von der Evaluierung ausgeschlossen. Die Kontrolle schlägt fehl, wenn Backups für die Instanz nicht aktiviert sind oder wenn die Aufbewahrungsdauer unter dem angegebenen Zeitraum liegt. Sofern Sie keinen benutzerdefinierten Parameterwert für die Aufbewahrungsdauer von Backups angeben, verwendet Security Hub einen Standardwert von 7 Tagen.

Backups helfen Ihnen, sich schneller nach einem Sicherheitsvorfall zu erholen, und stärken die Widerstandsfähigkeit Ihrer Systeme. Mit Amazon RDS können Sie tägliche Snapshots des gesamten Instance-Volumes konfigurieren. Weitere Informationen zu automatisierten Amazon RDS-Backups finden Sie unter [Arbeiten mit Backups](#) im Amazon RDS-Benutzerhandbuch.

Abhilfe

Informationen zum Aktivieren automatisierter Backups auf einer RDS-DB-Instance finden Sie unter [Automatisierte Backups aktivieren](#) im Amazon RDS-Benutzerhandbuch.

[RDS.12] Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15) NIST.800-53.r5 AC-3, (7), NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6

Kategorie: Schützen > Sichere Zugriffsverwaltung > Passwortlose Authentifizierung

Schweregrad: Mittel

Art der Ressource: AWS::RDS::DBCluster

AWS Config -Regel: [rds-cluster-iam-authentication-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob in einem Amazon RDS-DB-Cluster die IAM-Datenbankauthentifizierung aktiviert ist.

Die IAM-Datenbankauthentifizierung ermöglicht eine passwortlose Authentifizierung bei Datenbank-Instances. Die Authentifizierung verwendet ein Authentifizierungstoken. Der Netzwerkverkehr zur und von der Datenbank wird mit SSL verschlüsselt. Weitere Informationen finden Sie unter [IAM-Datenbank-Authentifizierung](#) im Amazon Aurora-Benutzerhandbuch.

Abhilfe

Informationen zur Aktivierung der IAM-Authentifizierung für einen DB-Cluster finden Sie unter [Aktivieren und Deaktivieren der IAM-Datenbankauthentifizierung](#) im Amazon Aurora Benutzerhandbuch.

[RDS.13] Automatische RDS-Upgrades für Nebenversionen sollten aktiviert sein

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/2.3.2, NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), NIST.800-53.R5 SI-2 (5), PCI DSS v4.0.1/6.3.3

Kategorie: Identifizieren > Sicherheitslücken-, Patch- und Versionsverwaltung

Schweregrad: Hoch

Art der Ressource: AWS::RDS::DBInstance

AWS Config -Regel: [rds-automatic-minor-version-upgrade-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob automatische Upgrades für kleinere Versionen für die RDS-Datenbank-Instance aktiviert sind.

Durch automatische Upgrades von Nebenversionen wird eine Datenbank regelmäßig auf die neuesten Versionen der Datenbank-Engine aktualisiert. Das Upgrade beinhaltet jedoch möglicherweise nicht immer die neueste Version der Datenbank-Engine. Wenn Sie Ihre Datenbanken zu bestimmten Zeiten auf bestimmten Versionen belassen müssen, empfehlen wir Ihnen, ein manuelles Upgrade auf die Datenbankversionen durchzuführen, die Sie gemäß Ihrem erforderlichen Zeitplan benötigen. Bei kritischen Sicherheitsproblemen oder wenn eine Version ihr end-of-support Datum erreicht, führt Amazon RDS möglicherweise ein Upgrade für eine Nebenversion durch, auch wenn Sie die Option Automatisches Upgrade der Nebenversion nicht aktiviert haben. Weitere Informationen finden Sie in der Amazon RDS-Upgrade-Dokumentation für Ihre spezifische Datenbank-Engine:

- [Automatische Nebenversions-Upgrades für RDS for MariaDB](#)
- [Automatische Upgrades kleinerer Versionen für RDS for MySQL](#)
- [Automatische Upgrades kleinerer Versionen für RDS for PostgreSQL](#)
- [Versionen von Db2 auf Amazon RDS](#)
- [Upgrades kleinerer Oracle-Versionen](#)
- [Upgrades der Microsoft SQL Server-DB-Engine](#)

Abhilfe

Informationen zur Aktivierung automatischer Unterversionen-Upgrades für eine bestehende DB-Instance finden Sie unter [Ändern einer Amazon RDS-DB-Instance](#) im Amazon RDS-Benutzerhandbuch. Wählen Sie für das automatische Upgrade der Nebenversion Ja aus.

[RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-6, NIST.800-53.R5 CP-6 (1), NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 CP-9, NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Backups aktiviert

Schweregrad: Mittel

Ressourcentyp: AWS::RDS::DBCluster

AWS Config -Regel: [aurora-mysql-backtracking-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert	
BacktrackWindowInHours	Anzahl der Stunden, um einen Aurora MySQL-Cluster zurückzuverfolgen	Double	0.1 auf 72	Kein Standardwert	

Dieses Steuerelement prüft, ob für einen Amazon Aurora Cluster Backtracking aktiviert ist. Die Steuerung schlägt fehl, wenn für den Cluster kein Backtracking aktiviert ist. Wenn Sie einen benutzerdefinierten Wert für den `BacktrackWindowInHours` Parameter angeben, ist die Steuerung nur erfolgreich, wenn der Cluster für den angegebenen Zeitraum zurückverfolgt wird.

Mithilfe von Backups können Sie sich nach einem Sicherheitsvorfall schneller erholen. Sie stärken auch die Widerstandsfähigkeit Ihrer Systeme. Aurora-Backtracking reduziert die Zeit für die Wiederherstellung einer Datenbank auf einen bestimmten Zeitpunkt. Dazu ist keine Datenbankwiederherstellung erforderlich.

Abhilfe

Informationen zur Aktivierung von Aurora-Backtracking finden Sie unter [Backtracking konfigurieren](#) im Amazon Aurora Benutzerhandbuch.

Beachten Sie, dass Sie Backtracking nicht auf einem vorhandenen Cluster aktivieren können. Stattdessen können Sie einen Clone erstellen, für den Backtracking aktiviert ist. Weitere Informationen zu den Einschränkungen von Aurora-Backtracking finden Sie in der Liste der Einschränkungen unter [Backtracking im Überblick](#).

[RDS.15] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: AWS::RDS::DBCluster

AWS Config -Regel: [rds-cluster-multi-az-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Hochverfügbarkeit für Ihre RDS-DB-Cluster aktiviert ist. Die Steuerung schlägt fehl, wenn ein RDS-DB-Cluster nicht in mehreren Availability Zones (AZs) bereitgestellt wird.

RDS-DB-Cluster sollten für mehrere konfiguriert werden AZs , um die Verfügbarkeit der gespeicherten Daten sicherzustellen. Die Bereitstellung auf mehreren AZs Geräten ermöglicht einen automatisierten Failover im Falle eines AZ-Verfügbarkeitsproblems und während regelmäßiger RDS-Wartungsereignisse.

Abhilfe

Um Ihre DB-Cluster in mehreren bereitzustellen AZs, [ändern Sie eine DB-Instance zu einer Multi-AZ-DB-Instance-Bereitstellung](#) im Amazon RDS-Benutzerhandbuch.

Die Schritte zur Behebung sind für globale Aurora-Datenbanken unterschiedlich. Um mehrere Availability Zones für eine globale Aurora-Datenbank zu konfigurieren, wählen Sie Ihren DB-Cluster aus. Wählen Sie dann Aktionen und Leser hinzufügen und geben Sie mehrere an AZs. Weitere Informationen finden Sie unter [Hinzufügen von Aurora Replicas zu einem DB-Cluster](#) im Amazon Aurora Benutzerhandbuch.

[RDS.16] Aurora-DB-Cluster sollten so konfiguriert sein, dass sie Tags in DB-Snapshots kopieren

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2)

Kategorie: Identifizieren > Bestand

Schweregrad: Niedrig

Art der Ressource: AWS::RDS::DBCluster

AWS Config Regel: rds-cluster-copy-tags-to-snapshots-enabled (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon Aurora Aurora-DB-Cluster so konfiguriert ist, dass Tags automatisch in Snapshots des DB-Clusters kopiert werden, wenn die Snapshots erstellt werden. Die Steuerung schlägt fehl, wenn der Aurora-DB-Cluster nicht so konfiguriert ist, dass Tags bei der Erstellung der Snapshots automatisch in Snapshots des Clusters kopiert werden.

Die Identifizierung und Inventarisierung Ihrer IT-Ressourcen ist ein entscheidender Aspekt der Unternehmensführung und Sicherheit. Sie benötigen einen Überblick über all Ihre Amazon Aurora Aurora-DB-Cluster, damit Sie deren Sicherheitslage beurteilen und Maßnahmen gegen potenzielle Schwachstellen ergreifen können. Aurora-DB-Snapshots sollten dieselben Tags wie ihre übergeordneten DB-Cluster haben. In Amazon Aurora können Sie einen DB-Cluster so konfigurieren, dass automatisch alle Tags für den Cluster in Snapshots des Clusters kopiert werden. Durch die Aktivierung dieser Einstellung wird sichergestellt, dass DB-Snapshots dieselben Tags erben wie ihre übergeordneten DB-Cluster.

Note

Am 30. Juni 2025 änderte Security Hub den Titel dieses Steuerelements. Zuvor lautete der Titel dieses Steuerelements: RDS DB clusters should be configured to copy tags to snapshots. Der neue Titel spiegelt genauer wider, dass die Steuerung nur Amazon Aurora Aurora-DB-Cluster überprüft.

Abhilfe

Informationen zur Konfiguration eines Amazon Aurora Aurora-DB-Clusters für das automatische Kopieren von Tags in DB-Snapshots finden Sie unter [Ändern eines Amazon Aurora Aurora-DB-Clusters](#) im Amazon Aurora Aurora-Benutzerhandbuch.

[RDS.17] RDS-DB-Instances sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2)

Kategorie: Identifizieren > Bestand

Schweregrad: Niedrig

Art der Ressource: AWS::RDS::DBInstance

AWS Config Regel: `rds-instance-copy-tags-to-snapshots-enabled` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob RDS-DB-Instances so konfiguriert sind, dass sie bei der Erstellung der Snapshots alle Tags in Snapshots kopieren.

Die Identifizierung und Inventarisierung Ihrer IT-Ressourcen ist ein entscheidender Aspekt der Unternehmensführung und Sicherheit. Sie benötigen einen Überblick über all Ihre RDS-DB-Instances, damit Sie deren Sicherheitslage beurteilen und Maßnahmen gegen potenzielle Schwachstellen ergreifen können. Snapshots sollten auf die gleiche Weise gekennzeichnet werden wie ihre übergeordneten RDS-Datenbank-Instances. Durch die Aktivierung dieser Einstellung wird sichergestellt, dass Snapshots die Tags ihrer übergeordneten Datenbank-Instances erben.

Abhilfe

Informationen zum automatischen Kopieren von Tags in Snapshots für eine RDS-DB-Instance finden Sie unter [Ändern einer Amazon RDS-DB-Instance](#) im Amazon RDS-Benutzerhandbuch. Wählen Sie Tags in Snapshots kopieren aus.

[RDS.18] RDS-Instances sollten in einer VPC bereitgestellt werden

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen in VPC

Schweregrad: Hoch

Art der Ressource: AWS::RDS::DBInstance

AWS Config Regel: `rds-deployed-in-vpc` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Amazon RDS-Instance auf einer EC2 VPC bereitgestellt ist.

VPCs bietet eine Reihe von Netzwerksteuerungen, um den Zugriff auf RDS-Ressourcen zu sichern. Diese Kontrollen umfassen VPC-Endpunkte ACLs, Netzwerk- und Sicherheitsgruppen. Um diese Steuerelemente nutzen zu können, empfehlen wir Ihnen, Ihre RDS-Instances auf einer EC2 VPC zu erstellen.

Abhilfe

Anweisungen zum Verschieben von RDS-Instances in eine VPC finden Sie unter [Aktualisieren der VPC für eine DB-Instance](#) im Amazon RDS-Benutzerhandbuch.

[RDS.19] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Cluster-Ereignisse konfiguriert werden

Verwandte Anforderungen:, NIST.800-53.R5 NIST.800-53.r5 CA-7 SI-2

Kategorie: Erkennen > Erkennungsdienste > Anwendungsüberwachung

Schweregrad: Niedrig

Art der Ressource: AWS::RDS::EventSubscription

AWS Config Regel: rds-cluster-event-notifications-configured (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob in einem bestehenden Amazon RDS-Ereignisabonnement für Datenbankcluster Benachrichtigungen für die folgenden Schlüssel-Wert-Paare aus Quelle und Ereigniskategorie aktiviert sind:

```
DBCluster: ["maintenance","failure"]
```

Die Kontrolle ist erfolgreich, wenn in Ihrem Konto keine Event-Abonnements vorhanden sind.

RDS-Ereignisbenachrichtigungen verwendet Amazon SNS, um Sie über Änderungen in der Verfügbarkeit oder Konfiguration Ihrer RDS-Ressourcen zu informieren. Diese Benachrichtigungen ermöglichen eine schnelle Reaktion. Weitere Informationen zu RDS-Ereignisbenachrichtigungen finden Sie unter [Verwenden von Amazon RDS-Ereignisbenachrichtigungen](#) im Amazon RDS-Benutzerhandbuch.

Abhilfe

Informationen zum Abonnieren von RDS-Cluster-Ereignisbenachrichtigungen finden Sie unter [Amazon RDS-Ereignisbenachrichtigungen abonnieren](#) im Amazon RDS-Benutzerhandbuch.

Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Source type (Quellentyp)	Cluster
Zu berücksichtigende Cluster	Alle Cluster
Zu berücksichtigende Veranstaltungskategorien	Wählen Sie bestimmte Veranstaltungskategorien oder Alle Veranstaltungskategorien

[RDS.20] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Ereignisse der Datenbankinstanz konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-2, PCI DSS v4.0.1/11.5.2

Kategorie: Erkennen > Erkennungsdienste > Anwendungsüberwachung

Schweregrad: Niedrig

Art der Ressource: AWS::RDS::EventSubscription

AWS Config Regel: rds-instance-event-notifications-configured (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob in einem bestehenden Amazon RDS-Ereignisabonnement für Datenbank-Instances Benachrichtigungen für die folgenden Schlüssel-Wert-Paare aus Quelltyp und Ereigniskategorie aktiviert sind:

DBInstance: ["maintenance","configuration change","failure"]

Die Kontrolle ist erfolgreich, wenn in Ihrem Konto keine Event-Abonnements vorhanden sind.

RDS-Ereignisbenachrichtigungen verwenden Amazon SNS, um Sie über Änderungen in der Verfügbarkeit oder Konfiguration Ihrer RDS-Ressourcen zu informieren. Diese Benachrichtigungen ermöglichen eine schnelle Reaktion. Weitere Informationen zu RDS-Ereignisbenachrichtigungen finden Sie unter [Verwenden von Amazon RDS-Ereignisbenachrichtigungen](#) im Amazon RDS-Benutzerhandbuch.

Abhilfe

Informationen zum Abonnieren von RDS-Instance-Ereignisbenachrichtigungen finden Sie unter [Amazon RDS-Ereignisbenachrichtigungen abonnieren](#) im Amazon RDS-Benutzerhandbuch.

Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Source type (Quellentyp)	Instances
Instances, die aufgenommen werden sollen	Alle Instanzen
Zu berücksichtigende Event-Kategorien	Wählen Sie bestimmte Veranstaltungskategorien oder Alle Veranstaltungskategorien

[RDS.21] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbankparametergruppenereignisse konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-2, PCI DSS v4.0.1/11.5.2

Kategorie: Erkennen > Erkennungsdienste > Anwendungsüberwachung

Schweregrad: Niedrig

Art der Ressource: AWS::RDS::EventSubscription

AWS Config Regel: rds-pg-event-notifications-configured (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon RDS-Ereignisabonnement mit aktivierten Benachrichtigungen für die folgenden Schlüsselwertpaare aus Quelltyp, Ereigniskategorie, aktiviert ist. Die Kontrolle ist erfolgreich, wenn in Ihrem Konto keine Event-Abonnements vorhanden sind.

```
DBParameterGroup: ["configuration change"]
```

RDS-Ereignisbenachrichtigungen verwenden Amazon SNS, um Sie über Änderungen in der Verfügbarkeit oder Konfiguration Ihrer RDS-Ressourcen zu informieren. Diese Benachrichtigungen ermöglichen eine schnelle Reaktion. Weitere Informationen zu RDS-Ereignisbenachrichtigungen finden Sie unter [Verwenden von Amazon RDS-Ereignisbenachrichtigungen](#) im Amazon RDS-Benutzerhandbuch.

Abhilfe

Informationen zum Abonnieren von Ereignisbenachrichtigungen für RDS-Datenbankparametergruppen finden Sie unter [Amazon RDS-Ereignisbenachrichtigungen abonnieren](#) im Amazon RDS-Benutzerhandbuch. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Source type (Quellentyp)	Parametergruppen
Zu berücksichtigende Parametergruppen	Alle Parametergruppen
Zu berücksichtigende Event-Kategorien	Wählen Sie bestimmte Veranstaltungskategorien oder Alle Veranstaltungskategorien

[RDS.22] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbanksicherheitsgruppenereignisse konfiguriert werden

Verwandte Anforderungen: NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-2, PCI DSS v4.0.1/11.5.2

Kategorie: Erkennen > Erkennungsdienste > Anwendungsüberwachung

Schweregrad: Niedrig

Art der Ressource: AWS::RDS::EventSubscription

AWS Config Regel: rds-sg-event-notifications-configured (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon RDS-Ereignisabonnement mit aktivierten Benachrichtigungen für die folgenden Schlüsselwertpaare aus Quelltyp, Ereigniskategorie, aktiviert ist. Die Kontrolle ist erfolgreich, wenn in Ihrem Konto keine Event-Abonnements vorhanden sind.

```
DBSecurityGroup: ["configuration change","failure"]
```

RDS-Ereignisbenachrichtigungen verwenden Amazon SNS, um Sie über Änderungen in der Verfügbarkeit oder Konfiguration Ihrer RDS-Ressourcen zu informieren. Diese Benachrichtigungen ermöglichen eine schnelle Reaktion. Weitere Informationen zu RDS-Ereignisbenachrichtigungen finden Sie unter [Verwenden von Amazon RDS-Ereignisbenachrichtigungen](#) im Amazon RDS-Benutzerhandbuch.

Abhilfe

Informationen zum Abonnieren von RDS-Instance-Ereignisbenachrichtigungen finden Sie unter [Amazon RDS-Ereignisbenachrichtigungen abonnieren](#) im Amazon RDS-Benutzerhandbuch.

Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Source type (Quellentyp)	Sicherheitsgruppen
Zu berücksichtigende Sicherheitsgruppen	Alle Sicherheitsgruppen
Zu berücksichtigende Event-Kategorien	Wählen Sie bestimmte Veranstaltungskategorien oder Alle Veranstaltungskategorien

[RDS.23] RDS-Instances sollten keinen Standard-Port für die Datenbank-Engine verwenden

Verwandte Anforderungen: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (5)

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Niedrig

Art der Ressource: AWS::RDS::DBInstance

AWS Config Regel: rds-no-default-ports (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein RDS-Cluster oder eine RDS-Instanz einen anderen Port als den Standardport der Datenbank-Engine verwendet. Die Steuerung schlägt fehl, wenn der RDS-Cluster oder die RDS-Instanz den Standardport verwendet. Diese Steuerung gilt nicht für RDS-Instances, die Teil eines Clusters sind.

Wenn Sie einen bekannten Port verwenden, um einen RDS-Cluster oder eine RDS-Instanz bereitzustellen, kann ein Angreifer Informationen über den Cluster oder die Instanz erraten. Der Angreifer kann diese Informationen in Verbindung mit anderen Informationen verwenden, um eine Verbindung zu einem RDS-Cluster oder einer RDS-Instanz herzustellen oder zusätzliche Informationen über Ihre Anwendung zu erhalten.

Wenn Sie den Port ändern, müssen Sie auch die vorhandenen Verbindungszeichenfolgen aktualisieren, die für die Verbindung mit dem alten Port verwendet wurden. Sie sollten auch die Sicherheitsgruppe der DB-Instanz überprüfen, um sicherzustellen, dass sie eine Eingangsregel enthält, die Konnektivität auf dem neuen Port ermöglicht.

Abhilfe

Informationen zum Ändern des Standardports einer vorhandenen RDS-DB-Instanz finden Sie unter [Ändern einer Amazon RDS-DB-Instanz](#) im Amazon RDS-Benutzerhandbuch. Informationen zum Ändern des Standardports eines vorhandenen RDS-DB-Clusters finden Sie unter [Ändern des DB-Clusters mithilfe der Konsole, der CLI und der API](#) im Amazon Aurora Benutzerhandbuch. Ändern Sie für den Datenbankport den Portwert auf einen Wert, der nicht dem Standard entspricht.

[RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2, PCI DSS v4.0.1/2.2.2

Kategorie: Identifizieren > Ressourcenkonfiguration

Schweregrad: Mittel

Art der Ressource: AWS::RDS::DBCluster

AWS Config -Regel: [rds-cluster-default-admin-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon RDS-Datenbank-Cluster den Standardwert des Admin-Benutzernamens geändert hat. Die Steuerung gilt nicht für Engines des Typs Neptune (Neptune DB) oder docdb (DocumentDB). Diese Regel schlägt fehl, wenn der Admin-Benutzername auf den Standardwert gesetzt ist.

Wenn Sie eine Amazon RDS-Datenbank erstellen, sollten Sie den standardmäßigen Administratorbenutzernamen in einen eindeutigen Wert ändern. Standardbenutzernamen sind allgemein bekannt und sollten bei der Erstellung der RDS-Datenbank geändert werden. Durch das Ändern der Standardbenutzernamen wird das Risiko eines unbeabsichtigten Zugriffs verringert.

Abhilfe

Um den Admin-Benutzernamen zu ändern, der mit dem Amazon RDS-Datenbank-Cluster verknüpft ist, [erstellen Sie einen neuen RDS-Datenbank-Cluster](#) und ändern Sie den Standard-Admin-Benutzernamen beim Erstellen der Datenbank.

[RDS.25] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2, PCI DSS v4.0.1/2.2.2

Kategorie: Identifizieren > Ressourcenkonfiguration

Schweregrad: Mittel

Art der Ressource: AWS::RDS::DBInstance

AWS Config -Regel: [rds-instance-default-admin-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Sie den Administrator-Benutzernamen für Amazon Relational Database Service (Amazon RDS) -Datenbank-Instances gegenüber dem Standardwert geändert haben. Die Steuerung schlägt fehl, wenn der Administrator-Benutzername auf den Standardwert

gesetzt ist. Die Steuerung gilt nicht für Engines des Typs Neptune (Neptune DB) oder docdb (DocumentDB) und für RDS-Instances, die Teil eines Clusters sind.

Standardmäßige Administratorbenutzernamen in Amazon RDS-Datenbanken sind allgemein bekannt. Wenn Sie eine Amazon RDS-Datenbank erstellen, sollten Sie den standardmäßigen Administratorbenutzernamen in einen eindeutigen Wert ändern, um das Risiko eines unbeabsichtigten Zugriffs zu verringern.

Abhilfe

Um den mit einer RDS-Datenbank-Instance verknüpften Administrator-Benutzernamen zu ändern, [erstellen Sie zunächst eine neue RDS-Datenbank-Instance](#). Ändern Sie den standardmäßigen Administratorbenutzernamen beim Erstellen der Datenbank.

[RDS.26] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden

Kategorie: Wiederherstellung > Ausfallsicherheit > Backups aktiviert

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-12, NIST.800-53.R5 SI-13 (5)

Schweregrad: Mittel

Art der Ressource: AWS::RDS::DBInstance

AWS Config Regel: [rds-resources-protected-by-backup-plan](#)

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Standardwert	
backupVaultLockCheck	Das Steuerelement gibt einen PASSED Befund aus, wenn der Parameter auf true gesetzt ist und	Boolesch	true oder false	Kein Standardwert	

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Standardwert	
	die Ressource AWS Backup Vault Lock verwendet.				

Diese Kontrolle bewertet, ob Amazon RDS-DB-Instances durch einen Backup-Plan abgedeckt sind. Diese Kontrolle schlägt fehl, wenn die RDS-DB-Instance nicht durch einen Backup-Plan abgedeckt ist. Wenn Sie den `backupVaultLockCheck` Parameter auf `gleich setzenttrue`, wird die Kontrolle nur erfolgreich ausgeführt, wenn die Instance in einem AWS Backup gesicherten Tresor gesichert ist.

AWS Backup ist ein vollständig verwalteter Backup-Service, der die gesamte Datensicherung zentralisiert und automatisiert. AWS-Services Mit können Sie Backup-Richtlinien erstellen AWS Backup, die als Backup-Pläne bezeichnet werden. Mit diesen Plänen können Sie Ihre Sicherungsanforderungen definieren, z. B. wie häufig Ihre Daten gesichert werden sollen und wie lange diese Sicherungen aufbewahrt werden sollen. Durch die Aufnahme von RDS-DB-Instances in einen Backup-Plan können Sie Ihre Daten vor unbeabsichtigtem Verlust oder Löschung schützen.

Abhilfe

Informationen zum Hinzufügen einer RDS-DB-Instance zu einem AWS Backup Backup-Plan finden Sie unter [Zuweisen von Ressourcen zu einem Backup-Plan](#) im AWS Backup Entwicklerhandbuch.

[RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), (10), NIST.800-53.R5 SI-7 NIST.800-53.r5 SC-7 (6)

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config Regel: [rds-cluster-encrypted-at-rest](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein RDS-DB-Cluster im Ruhezustand verschlüsselt ist. Die Steuerung schlägt fehl, wenn ein RDS-DB-Cluster im Ruhezustand nicht verschlüsselt ist.

Daten im Ruhezustand beziehen sich auf alle Daten, die für einen beliebigen Zeitraum in einem persistenten, nichtflüchtigen Speicher gespeichert werden. Durch Verschlüsselung können Sie die Vertraulichkeit solcher Daten schützen und so das Risiko verringern, dass ein unberechtigter Benutzer darauf zugreifen kann. Die Verschlüsselung Ihrer RDS-DB-Cluster schützt Ihre Daten und Metadaten vor unbefugtem Zugriff. Es erfüllt auch die Compliance-Anforderungen für die data-at-rest Verschlüsselung von Produktionsdateisystemen.

Abhilfe

Sie können die Verschlüsselung im Ruhezustand aktivieren, wenn Sie einen RDS-DB-Cluster erstellen. Sie können die Verschlüsselungseinstellungen nach dem Erstellen eines Clusters nicht ändern. Weitere Informationen finden Sie unter [Verschlüsseln eines Amazon Aurora Aurora-DB-Clusters](#) im Amazon Aurora Aurora-Benutzerhandbuch.

[RDS.28] RDS-DB-Cluster sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::RDS::DBCluster

AWS Config Regel: tagged-rds-dbccluster (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
requiredTagKeys	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS	Kein Standardwert

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen.	

Dieses Steuerelement prüft, ob ein Amazon RDS-DB-Cluster Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind `requiredTagKeys`. Die Steuerung schlägt fehl, wenn der DB-Cluster keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der DB-Cluster mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `aws:` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der Allgemeinen AWS-Referenz.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem RDS-DB-Cluster finden Sie unter [Tagging Amazon RDS-Ressourcen](#) im Amazon RDS-Benutzerhandbuch.

[RDS.29] RDS-DB-Cluster-Snapshots sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::RDS::DBClusterSnapshot

AWS Config Regel: tagged-rds-dbclustersnapshot (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
requiredTagKeys	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon RDS-DB-Cluster-Snapshot Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind `requiredTagKeys`. Die Steuerung schlägt fehl, wenn der DB-Cluster-Snapshot keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der DB-Cluster-Snapshot mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem RDS-DB-Cluster-Snapshot finden Sie unter [Tagging Amazon RDS-Ressourcen](#) im Amazon RDS-Benutzerhandbuch.

[RDS.30] RDS-DB-Instances sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::RDS::DBInstance

AWS Config Regel: tagged-rds-dbinstance (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon RDS-DB-Instance Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind `requiredTagKeys`. Die Kontrolle schlägt fehl, wenn die DB-Instance keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die DB-Instance mit keinem Schlüssel gekennzeichnet ist. System-Tags, die automatisch angewendet werden und mit `aws:*` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer RDS-DB-Instance finden Sie unter [Tagging Amazon RDS-Ressourcen](#) im Amazon RDS-Benutzerhandbuch.

[RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBSecurityGroup`

AWS Config Regel: `tagged-rds-dbsecuritygroup` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon RDS-DB-Sicherheitsgruppe Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind `requiredTagKeys`. Die Kontrolle schlägt fehl, wenn die DB-Sicherheitsgruppe keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die DB-Sicherheitsgruppe mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer RDS-DB-Sicherheitsgruppe finden Sie unter [Tagging Amazon RDS-Ressourcen](#) im Amazon RDS-Benutzerhandbuch.

[RDS.32] RDS-DB-Snapshots sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::RDS::DBSnapshot

AWS Config Regel: tagged-rds-dbsnapshot (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
requiredTagKeys	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon RDS-DB-Snapshot Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind `requiredTagKeys`. Die Steuerung schlägt fehl, wenn der DB-Snapshot keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der DB-Snapshot mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `aws:` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien

für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem RDS-DB-Snapshot finden Sie unter [Tagging Amazon RDS-Ressourcen](#) im Amazon RDS-Benutzerhandbuch.

[RDS.33] RDS-DB-Subnetzgruppen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::RDS::DBSubnetGroup

AWS Config Regel: tagged-rds-dbsubnetgroups (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
requiredTagKeys	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS	Kein Standardwert

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen.	

Dieses Steuerelement prüft, ob eine Amazon RDS-DB-Subnetzgruppe Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn die DB-Subnetzgruppe keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat. `requiredTagKeys` Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die DB-Subnetzgruppe mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` , werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer RDS-DB-Subnetzgruppe finden Sie unter [Tagging Amazon RDS-Ressourcen](#) im Amazon RDS-Benutzerhandbuch.

[RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 (9), NIST.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8), PCI DSS v4.0.1/10.2.1 NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Ressourcentyp: AWS::RDS::DBCluster

AWS Config Regel: [rds-aurora-mysql-audit-logging-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob ein Amazon Aurora MySQL-DB-Cluster so konfiguriert ist, dass er Audit-Logs in Amazon CloudWatch Logs veröffentlicht. Die Steuerung schlägt fehl, wenn der Cluster nicht für die Veröffentlichung von Audit-Logs in Logs konfiguriert ist. CloudWatch Das Steuerelement generiert keine Ergebnisse für Aurora Serverless v1-DB-Cluster.

In Audit-Logs werden Datenbankaktivitäten aufgezeichnet, darunter Anmeldeversuche, Datenänderungen, Schemaänderungen und andere Ereignisse, die aus Sicherheits- und Compliance-Gründen geprüft werden können. Wenn Sie einen Aurora MySQL-DB-Cluster so konfigurieren, dass er Audit-Logs in einer Protokollgruppe in Amazon CloudWatch Logs veröffentlicht, können Sie eine Echtzeitanalyse der Protokolldaten durchführen. CloudWatch Logs speichert Protokolle in einem äußerst langlebigen Speicher. Sie können auch Alarme erstellen und Messwerte in anzeigen CloudWatch.

Note

Eine alternative Möglichkeit, Audit-Logs in Logs zu CloudWatch veröffentlichen, besteht darin, die erweiterte Überwachung zu aktivieren und den DB-Parameter

`server_audit_logs_upload` auf Clusterebene auf zu setzen. 1 Die Standardeinstellung für `server_audit_logs_upload` parameter. 0 Wir empfehlen jedoch, stattdessen die folgenden Anweisungen zur Problembehebung zu verwenden, um diese Kontrolle zu bestehen.

Abhilfe

Informationen zum Veröffentlichen von Aurora CloudWatch MySQL-DB-Cluster-Prüfprotokollen in Logs finden Sie unter [Veröffentlichen von Amazon Aurora CloudWatch MySQL-Protokollen in Amazon Logs](#) im Amazon Aurora Benutzerhandbuch.

[RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), NIST.800-53.R5 SI-2 (5), PCI DSS v4.0.1/6.3.3

Kategorie: Identifizieren > Sicherheitslücken-, Patch- und Versionsverwaltung

Schweregrad: Mittel

Art der Ressource: AWS::RDS::DBCluster

AWS Config Regel: [rds-cluster-auto-minor-version-upgrade-enable](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob das automatische Upgrade einer Nebenversion für einen Amazon RDS-Multi-AZ-DB-Cluster aktiviert ist. Die Steuerung schlägt fehl, wenn das automatische Upgrade der Nebenversion für den Multi-AZ-DB-Cluster nicht aktiviert ist.

RDS bietet ein automatisches Upgrade der Nebenversion, sodass Sie Ihren Multi-AZ-DB-Cluster auf dem neuesten Stand halten können. Nebenversionen können neue Softwarefunktionen, Bugfixes, Sicherheitspatches und Leistungsverbesserungen einführen. Durch die Aktivierung des automatischen Upgrades für Nebenversionen auf RDS-Datenbankclustern erhält der Cluster zusammen mit den Instances im Cluster automatische Updates für die Nebenversion, sobald

neue Versionen verfügbar sind. Die Updates werden während des Wartungsfensters automatisch angewendet.

Abhilfe

Informationen zur Aktivierung des automatischen Upgrades auf Multi-AZ-DB-Clustern finden Sie unter [Ändern eines Multi-AZ-DB-Clusters](#) im Amazon RDS-Benutzerhandbuch.

[RDS.36] RDS für PostgreSQL-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch

Verwandte Anforderungen: PCI DSS v4.0.1/10.4.2

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS::RDS::DBInstance

AWS Config -Regel: [rds-postgresql-logs-to-cloudwatch](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
logTypes	Durch Kommas getrennte Liste der Protokolltypen, die in Logs veröffentlicht werden sollen CloudWatch	StringList	Nicht anpassbar	postgresql

Dieses Steuerelement prüft, ob eine Amazon RDS for PostgreSQL PostgreSQL-DB-Instance für die Veröffentlichung von Protokollen in Amazon CloudWatch Logs konfiguriert ist. Die Steuerung schlägt fehl, wenn die PostgreSQL-DB-Instance nicht so konfiguriert ist, dass sie die im logTypes Parameter genannten Protokolltypen in Logs veröffentlicht. CloudWatch

Die Datenbankprotokollierung liefert detaillierte Aufzeichnungen von Anfragen, die an eine RDS-Instance gestellt wurden. PostgreSQL generiert Ereignisprotokolle, die nützliche Informationen für Administratoren enthalten. Durch die Veröffentlichung dieser CloudWatch Protokolle in Logs wird die Protokollverwaltung zentralisiert und Sie können die Protokolldaten in Echtzeit analysieren. CloudWatch Logs speichert die Protokolle in einem äußerst langlebigen Speicher. Sie können auch Alarme erstellen und Messwerte in anzeigenCloudWatch.

Abhilfe

Informationen zum Veröffentlichen von CloudWatch PostgreSQL-DB-Instance-Protokollen in Logs finden Sie unter [PostgreSQL-Protokolle in Amazon CloudWatch Logs veröffentlichen im Amazon RDS-Benutzerhandbuch](#).

[RDS.37] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch

Verwandte Anforderungen: PCI DSS v4.0.1/10.4.2

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS::RDS::DBCluster

AWS Config -Regel: [rds-aurora-postgresql-logs-to-cloudwatch](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon Aurora PostgreSQL-DB-Cluster für die Veröffentlichung von Protokollen in Amazon CloudWatch Logs konfiguriert ist. Die Steuerung schlägt fehl, wenn der Aurora PostgreSQL-DB-Cluster nicht für die Veröffentlichung von PostgreSQL-Protokollen in Logs konfiguriert ist. CloudWatch

Die Datenbankprotokollierung bietet detaillierte Aufzeichnungen von Anfragen, die an einen RDS-Cluster gestellt wurden. Aurora PostgreSQL generiert Ereignisprotokolle, die nützliche Informationen für Administratoren enthalten. Durch die Veröffentlichung dieser CloudWatch Protokolle in Logs wird die Protokollverwaltung zentralisiert und Sie können die Protokolldaten in Echtzeit analysieren. CloudWatch Logs speichert die Protokolle in einem äußerst langlebigen Speicher. Sie können auch Alarme erstellen und Messwerte in anzeigen CloudWatch.

Abhilfe

Informationen zum Veröffentlichen von Aurora CloudWatch PostgreSQL-DB-Cluster-Protokollen in Logs finden Sie unter [Veröffentlichen von Aurora PostgreSQL-Protokollen in Amazon CloudWatch Logs](#) im Amazon RDS-Benutzerhandbuch.

[RDS.38] RDS für PostgreSQL-DB-Instances sollten bei der Übertragung verschlüsselt werden

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: AWS::RDS::DBInstance

AWS Config -Regel: [rds-postgres-instance-encrypted-in-transit](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob eine Verbindung zu einer Amazon RDS for PostgreSQL Datenbank-Instance (DB) während der Übertragung verschlüsselt ist. Die Steuerung schlägt fehl, wenn der `rds.force_ssl` Parameter für die der Instance zugeordnete Parametergruppe auf `0` (aus) gesetzt ist. Dieses Steuerelement bewertet keine RDS-DB-Instances, die Teil eines DB-Clusters sind.

Daten während der Übertragung beziehen sich auf Daten, die von einem Standort an einen anderen übertragen werden, z. B. zwischen Knoten in Ihrem Cluster oder zwischen Ihrem Cluster und Ihrer Anwendung. Daten können über das Internet oder innerhalb eines privaten Netzwerks übertragen werden. Durch die Verschlüsselung von Daten während der Übertragung wird das Risiko verringert, dass ein nicht autorisierter Benutzer den Netzwerkverkehr abhören kann.

Abhilfe

Informationen dazu, dass alle Verbindungen zu Ihrer RDS for PostgreSQL-DB-Instance SSL verwenden müssen, finden Sie unter [Verwenden von SSL mit einer PostgreSQL-DB-Instance](#) im Amazon RDS-Benutzerhandbuch.

[RDS.39] RDS für MySQL-DB-Instances sollten bei der Übertragung verschlüsselt werden

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: AWS::RDS::DBInstance

AWS Config -Regel: [rds-mysql-instance-encrypted-in-transit](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob eine Verbindung zu einer Amazon RDS for MySQL Datenbank-Instance (DB) während der Übertragung verschlüsselt ist. Die Steuerung schlägt fehl, wenn der `rds.require_secure_transport` Parameter für die der Instance zugeordnete Parametergruppe auf `0` (aus) gesetzt ist. Dieses Steuerelement bewertet keine RDS-DB-Instances, die Teil eines DB-Clusters sind.

Daten während der Übertragung beziehen sich auf Daten, die von einem Standort an einen anderen übertragen werden, z. B. zwischen Knoten in Ihrem Cluster oder zwischen Ihrem Cluster und Ihrer Anwendung. Daten können über das Internet oder innerhalb eines privaten Netzwerks übertragen werden. Durch die Verschlüsselung von Daten während der Übertragung wird das Risiko verringert, dass ein nicht autorisierter Benutzer den Netzwerkverkehr abhören kann.

Abhilfe

Informationen dazu, dass alle Verbindungen zu Ihrer RDS for MySQL-DB-Instance SSL verwenden müssen, finden Sie unter [SSL/TLS-Unterstützung für MySQL-DB-Instances auf Amazon RDS](#) im Amazon RDS-Benutzerhandbuch.

[RDS.40] RDS für SQL Server-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), (10), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 NIST.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS::RDS::DBInstance

AWS Config -Regel: [rds-sql-server-logs-to-cloudwatch](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
logTypes	Eine Liste der Protokolltypen, für deren Veröffentlichung eine RDS for SQL Server-DB-Instance in CloudWatch Logs konfiguriert werden sollte. Diese Steuerung schlägt fehl, wenn eine DB-Instance nicht für die Veröffentlichung eines in der Liste angegebenen Protokolltyps konfiguriert ist.	EnumList (maximal 2 Elemente)	agent, error	agent, error

Dieses Steuerelement prüft, ob eine Amazon RDS for Microsoft SQL Server-DB-Instance für die Veröffentlichung von Protokollen in Amazon CloudWatch Logs konfiguriert ist. Die Steuerung schlägt fehl, wenn die RDS for SQL Server-DB-Instance nicht für die Veröffentlichung von Protokollen in CloudWatch Logs konfiguriert ist. Sie können optional die Protokolltypen angeben, für deren Veröffentlichung eine DB-Instance konfiguriert werden soll.

Die Datenbankprotokollierung bietet detaillierte Aufzeichnungen von Anfragen, die an eine Amazon RDS-DB-Instance gestellt wurden. Durch die Veröffentlichung von CloudWatch Protokollen in Logs wird die Protokollverwaltung zentralisiert und Sie können Protokolldaten in Echtzeit analysieren. CloudWatch Logs speichert Protokolle in einem äußerst langlebigen Speicher. Darüber hinaus können Sie damit Alarme für bestimmte Fehler erstellen, die auftreten können, z. B. bei häufigen Neustarts, die in einem Fehlerprotokoll aufgezeichnet werden. Ebenso können Sie Alarme für Fehler oder Warnungen erstellen, die in SQL Server-Agent-Protokollen aufgezeichnet werden, die sich auf SQL-Agent-Jobs beziehen.

Abhilfe

Informationen zum Veröffentlichen von Protokollen in CloudWatch Logs für eine RDS for SQL Server-DB-Instance finden Sie in den [Datenbankprotokolldateien von Amazon RDS for Microsoft SQL Server](#) im Amazon Relational Database Service User Guide.

[RDS.41] RDS für SQL Server-DB-Instances sollten bei der Übertragung verschlüsselt werden

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: AWS::RDS::DBInstance

AWS Config -Regel: [rds-sqlserver-encrypted-in-transit](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob eine Verbindung zu einer Amazon RDS for Microsoft SQL Server-DB-Instance während der Übertragung verschlüsselt ist. Die Steuerung schlägt fehl, wenn der `rds.force_ssl` Parameter der Parametergruppe, die der DB-Instance zugeordnet ist, auf `gesetzt` (off) ist.

Daten während der Übertragung beziehen sich auf Daten, die von einem Standort an einen anderen übertragen werden, z. B. zwischen Knoten in einem DB-Cluster oder zwischen einem DB-Cluster und einer Client-Anwendung. Daten können über das Internet oder innerhalb eines privaten Netzwerks übertragen werden. Durch die Verschlüsselung von Daten während der Übertragung wird das Risiko verringert, dass unbefugte Benutzer den Netzwerkverkehr abhören.

Abhilfe

Informationen SSL/TLS zur Aktivierung von Verbindungen zu Amazon RDS-DB-Instances, auf denen Microsoft SQL Server ausgeführt wird, finden Sie [unter Verwenden von SSL mit einer Microsoft SQL Server-DB-Instance](#) im Amazon Relational Database Service Service-Benutzerhandbuch.

[RDS.42] RDS für MariaDB-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), (9), NIST.800-53.r5 AC-6 (10) NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 NIST.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS::RDS::DBInstance

AWS Config -Regel: [mariadb-publish-logs-to-cloudwatch-logs](#)

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
logTypes	Eine Liste der Protokolltypen, für deren Veröffentlichung eine MariaDB-DB-Instance in Logs konfiguriert werden sollte. CloudWatch Das Steuerelement generiert einen FAILED Befund, wenn eine DB-Instance nicht für die Veröffentlichung eines in der Liste angegebenen Protokolltyps konfiguriert ist.	EnumList (maximal 4 Elemente)	audit, error, general, slowquery	audit, error

Dieses Steuerelement prüft, ob eine Amazon RDS for MariaDB-DB-Instance so konfiguriert ist, dass sie bestimmte Protokolltypen in Amazon CloudWatch Logs veröffentlicht. Die Steuerung schlägt fehl, wenn die MariaDB-DB-Instance nicht so konfiguriert ist, dass sie die Protokolle in Logs veröffentlicht. CloudWatch Sie können optional angeben, für welche Arten von Protokollen eine MariaDB-DB-Instance für die Veröffentlichung konfiguriert werden soll.

Die Datenbankprotokollierung bietet detaillierte Aufzeichnungen von Anfragen, die an eine Amazon RDS for MariaDB-DB-Instance gestellt wurden. Durch die Veröffentlichung von CloudWatch Protokollen in Amazon Logs wird die Protokollverwaltung zentralisiert und Sie können die Protokolldaten in Echtzeit analysieren. Darüber hinaus bewahrt CloudWatch Logs die Protokolle dauerhaft auf, sodass Sicherheits-, Zugriffs- und Verfügbarkeitsprüfungen und Audits unterstützt werden können. Mit CloudWatch Logs können Sie auch Alarme erstellen und Messwerte überprüfen.

Abhilfe

Informationen zur Konfiguration einer Amazon RDS for MariaDB-DB-Instance zur Veröffentlichung von Protokollen in Amazon CloudWatch Logs finden Sie unter [Veröffentlichen von MariaDB-Protokollen in Amazon Logs im Amazon CloudWatch](#) Relational Database Service Service-Benutzerhandbuch.

[RDS.44] RDS für MariaDB-DB-Instances sollte bei der Übertragung verschlüsselt werden

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: AWS::RDS::DBInstance

AWS Config -Regel: [rds-mariadb-instance-encrypted-in-transit](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob Verbindungen zu einer Amazon RDS for MariaDB-DB-Instance während der Übertragung verschlüsselt werden. Die Steuerung schlägt fehl, wenn die der DB-Instance zugeordnete DB-Parametergruppe nicht synchron ist oder der `require_secure_transport` Parameter der Parametergruppe nicht auf `gesetzt` ist. `ON`

 Note

Dieses Steuerelement bewertet keine Amazon RDS-DB-Instances, die MariaDB-Versionen vor Version 10.5 verwenden. Der `require_secure_transport` Parameter wird nur für MariaDB-Versionen 10.5 und höher unterstützt.

Daten während der Übertragung beziehen sich auf Daten, die von einem Ort zu einem anderen übertragen werden, z. B. zwischen Knoten in einem DB-Cluster oder zwischen einem DB-Cluster und einer Client-Anwendung. Daten können über das Internet oder innerhalb eines privaten Netzwerks übertragen werden. Durch die Verschlüsselung von Daten während der Übertragung wird das Risiko verringert, dass unbefugte Benutzer den Netzwerkverkehr abhören.

Abhilfe

Informationen zur Aktivierung SSL/TLS von Verbindungen zu einer Amazon RDS for MariaDB-DB-Instance finden Sie unter Required [SSL/TLS for all connections to a MariaDB DB Instance](#) im Amazon Relational Database Service User Guide.

[RDS.45] Bei Aurora MySQL-DB-Clustern sollte die Audit-Protokollierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 CA-7 NIST.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: [aurora-mysql-cluster-audit-logging](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob für einen Amazon Aurora MySQL-DB-Cluster die Audit-Protokollierung aktiviert ist. Die Kontrolle schlägt fehl, wenn die dem DB-Cluster zugeordnete DB-

Parametergruppe nicht synchron ist, der `server_audit_logging` Parameter nicht auf 1 gesetzt ist oder der `server_audit_events` Parameter auf einen leeren Wert gesetzt ist.

Datenbankprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen. In Auditprotokollen werden Datenbankaktivitäten aufgezeichnet, darunter Anmeldeversuche, Datenänderungen, Schemaänderungen und andere Ereignisse, die aus Sicherheits- und Compliance-Gründen überprüft werden können.

Abhilfe

Informationen zur Aktivierung der Protokollierung für einen Amazon Aurora MySQL-DB-Cluster finden Sie unter [Veröffentlichen von Amazon Aurora CloudWatch MySQL-Protokollen in Amazon Logs](#) im Amazon Aurora Aurora-Benutzerhandbuch.

Security Hub-Steuerelemente für Amazon Redshift

Diese AWS Security Hub Kontrollen bewerten den Service und die Ressourcen von Amazon Redshift. Die Steuerelemente sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[Redshift.1] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten

Verwandte Anforderungen: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.6, PCI DSS v4.0.1/1.4.4

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Kritisch

Art der Ressource: `AWS::Redshift::Cluster`

AWS Config -Regel: [redshift-cluster-public-access-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Amazon Redshift Redshift-Cluster öffentlich zugänglich sind. Es wertet das `PubliclyAccessible` Feld im Cluster-Konfigurationselement aus.

Das `PubliclyAccessible` Attribut der Amazon Redshift Redshift-Cluster-Konfiguration gibt an, ob der Cluster öffentlich zugänglich ist. Wenn der Cluster mit „`PubliclyAccessible` gesetzt auf“ konfiguriert ist `true`, handelt es sich um eine mit dem Internet verbundene Instance mit einem öffentlich auflösbaren DNS-Namen, der in eine öffentliche IP-Adresse aufgelöst wird.

Wenn der Cluster nicht öffentlich zugänglich ist, handelt es sich um eine interne Instanz mit einem DNS-Namen, der in eine private IP-Adresse aufgelöst wird. Sofern Sie nicht beabsichtigen, dass Ihr Cluster öffentlich zugänglich ist, sollte der Cluster nicht mit der `PubliclyAccessible` Einstellung auf `true` konfiguriert werden.

Abhilfe

Informationen zum Aktualisieren eines Amazon Redshift-Clusters zur Deaktivierung des öffentlichen Zugriffs finden Sie unter [Modifizieren eines Clusters](#) im Amazon Redshift Management Guide. Stellen Sie Öffentlich zugänglich auf Nein ein.

[Redshift.2] Verbindungen zu Amazon Redshift Redshift-Clustern sollten bei der Übertragung verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 3, 3 (NIST.800-53.r5 SC-23), NIST.800-53.r5 SC-2 (4),, NIST.800-53.r5 SC-7 (1), NIST.800-53.r5 SC-8 (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 PCI DSS v4.0.1/4.2.1

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: `AWS::Redshift::Cluster` `AWS::Redshift::ClusterParameterGroup`

AWS Config -Regel: [redshift-require-tls-ssl](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Verbindungen zu Amazon Redshift Redshift-Clustern erforderlich sind, um Verschlüsselung bei der Übertragung zu verwenden. Die Prüfung schlägt fehl, wenn der Amazon Redshift Redshift-Clusterparameter `require_SSL` nicht auf `True` gesetzt ist.

TLS kann verwendet werden, um zu verhindern, dass potenzielle Angreifer person-in-the-middle oder ähnliche Angriffe verwenden, um den Netzwerkverkehr zu belauschen oder zu manipulieren. Nur verschlüsselte Verbindungen über TLS sollten zugelassen werden. Das Verschlüsseln von Daten während der Übertragung kann die Leistung beeinträchtigen. Sie sollten Ihre Anwendung mit dieser Funktion testen, um das Leistungsprofil und die Auswirkungen von TLS zu verstehen.

Abhilfe

Informationen zum Aktualisieren einer Amazon Redshift-Parametergruppe, sodass eine Verschlüsselung erforderlich ist, finden Sie unter [Ändern einer Parametergruppe](#) im Amazon Redshift Management Guide. Auf True setzen **require_ssl**.

[Redshift.3] Bei Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), (10), NIST.800-53.r5 SC-7 NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Backups aktiviert

Schweregrad: Mittel

Ressourcentyp: AWS::Redshift::Cluster

AWS Config -Regel: [redshift-backup-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Standardwert	
MinRetentionPeriod	Minimale Aufbewahrungsdauer für Snapshots in Tagen	Ganzzahl	7 auf 35	7	

Dieses Steuerelement prüft, ob in einem Amazon Redshift Redshift-Cluster automatische Snapshots aktiviert sind und ob eine Aufbewahrungsdauer größer oder gleich dem angegebenen Zeitraum ist. Die Kontrolle schlägt fehl, wenn automatische Snapshots für den Cluster nicht aktiviert sind oder wenn die Aufbewahrungsdauer den angegebenen Zeitraum unterschreitet. Sofern Sie keinen benutzerdefinierten Parameterwert für die Aufbewahrungsdauer von Snapshots angeben, verwendet Security Hub einen Standardwert von 7 Tagen.

Mithilfe von Backups können Sie sich nach einem Sicherheitsvorfall schneller erholen. Sie stärken die Widerstandsfähigkeit Ihrer Systeme. Amazon Redshift erstellt standardmäßig regelmäßig Snapshots. Dieses Steuerelement prüft, ob automatische Snapshots aktiviert sind und mindestens sieben Tage lang aufbewahrt werden. Weitere Informationen zu automatisierten Amazon Redshift-Snapshots finden Sie unter [Automatisierte Snapshots](#) im Amazon Redshift Management Guide.

Abhilfe

Informationen zur Aktualisierung der Aufbewahrungsdauer von Snapshots für einen Amazon Redshift-Cluster finden Sie unter [Modifizieren eines Clusters](#) im Amazon Redshift Management Guide. Stellen Sie für Backup die Snapshot-Aufbewahrung auf einen Wert von 7 oder höher ein.

[Redshift.4] Bei Amazon Redshift Redshift-Clustern sollte die Auditprotokollierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), (9), NIST.800-53.r5 AC-6 NIST.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8), PCI DSS v4.0.1/10.2.1

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS::Redshift::Cluster

AWS Config Regel: redshift-cluster-audit-logging-enabled (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

- `loggingEnabled = true`(nicht anpassbar)

Dieses Steuerelement prüft, ob für einen Amazon Redshift Redshift-Cluster die Audit-Protokollierung aktiviert ist.

Die Amazon Redshift Redshift-Audit-Protokollierung bietet zusätzliche Informationen über Verbindungen und Benutzeraktivitäten in Ihrem Cluster. Diese Daten können in Amazon S3 gespeichert und gesichert werden und können bei Sicherheitsüberprüfungen und Untersuchungen hilfreich sein. Weitere Informationen finden Sie unter [Protokollierung von Datenbankprüfungen](#) im Amazon Redshift Management Guide.

Abhilfe

Informationen zur Konfiguration der Audit-Protokollierung für einen Amazon Redshift-Cluster finden Sie unter [Konfiguration der Überwachung mithilfe der Konsole](#) im Amazon Redshift Management Guide.

[Redshift.6] Bei Amazon Redshift sollten automatische Upgrades auf Hauptversionen aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), NIST.800-53.R5 SI-2 (5)

Kategorie: Identifizieren > Sicherheitslücken-, Patch- und Versionsverwaltung

Schweregrad: Mittel

Art der Ressource: AWS::Redshift::Cluster

AWS Config -Regel: [redshift-cluster-maintenancesettings-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- allowVersionUpgrade = true(nicht anpassbar)

Dieses Steuerelement prüft, ob automatische Hauptversions-Upgrades für den Amazon Redshift Redshift-Cluster aktiviert sind.

Durch die Aktivierung automatischer Hauptversions-Upgrades wird sichergestellt, dass die neuesten Hauptversionsupdates für Amazon Redshift Redshift-Cluster während des Wartungsfensters

installiert werden. Diese Updates können Sicherheitspatches und Bugfixes enthalten. Es ist ein wichtiger Schritt zur Sicherung von Systemen, über die Installation von Patches auf dem Laufenden zu bleiben.

Abhilfe

Um dieses Problem von zu beheben AWS CLI, verwenden Sie den Amazon Redshift `modify-cluster` Redshift-Befehl und legen Sie das `--allow-version-upgrade` Attribut fest. `clustername` ist der Name Ihres Amazon Redshift Redshift-Clusters.

```
aws redshift modify-cluster --cluster-identifier clustername --allow-version-upgrade
```

[Redshift.7] Redshift-Cluster sollten erweitertes VPC-Routing verwenden

Verwandte Anforderungen: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), (11) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SC-7

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Privater API-Zugriff

Schweregrad: Mittel

Art der Ressource: `AWS::Redshift::Cluster`

AWS Config -Regel: [redshift-enhanced-vpc-routing-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon Redshift Redshift-Cluster EnhancedVpcRouting aktiviert wurde.

Durch das verbesserte VPC-Routing wird der gesamte COPY UNLOAD Datenverkehr zwischen dem Cluster und den Datenrepositorys über Ihre VPC geleitet. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können VPC Flow Logs auch verwenden, um den Netzwerkverkehr zu überwachen.

Abhilfe

Detaillierte Anweisungen zur Problembehebung finden Sie unter [Enabling enhanced VPC Routing](#) im Amazon Redshift Management Guide.

[Redshift.8] Amazon Redshift Redshift-Cluster sollten nicht den standardmäßigen Admin-Benutzernamen verwenden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Identifizieren > Ressourcenkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::Redshift::Cluster`

AWS Config -Regel: [redshift-default-admin-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon Redshift Redshift-Cluster den Standardwert des Admin-Benutzernamens geändert hat. Diese Steuerung schlägt fehl, wenn der Admin-Benutzername für einen Redshift-Cluster auf `awsuser` gesetzt ist.

Wenn Sie einen Redshift-Cluster erstellen, sollten Sie den Standard-Administratorbenutzernamen in einen eindeutigen Wert ändern. Standardbenutzernamen sind allgemein bekannt und sollten bei der Konfiguration geändert werden. Durch das Ändern der Standardbenutzernamen wird das Risiko eines unbeabsichtigten Zugriffs verringert.

Abhilfe

Sie können den Admin-Benutzernamen für Ihren Amazon Redshift Redshift-Cluster nicht ändern, nachdem Sie ihn erstellt haben. Informationen zum Erstellen eines neuen Clusters mit einem nicht standardmäßigen Benutzernamen finden Sie unter [Schritt 1: Erstellen eines Amazon Redshift-Beispielclusters im Amazon Redshift Getting Started Guide](#).

[Redshift.9] Redshift-Cluster sollten nicht den Standard-Datenbanknamen verwenden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Identifizieren > Ressourcenkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::Redshift::Cluster`

AWS Config -Regel: [redshift-default-db-name-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon Redshift Redshift-Cluster den Datenbanknamen gegenüber seinem Standardwert geändert hat. Die Steuerung schlägt fehl, wenn der Datenbankname für einen Redshift-Cluster auf dev gesetzt ist.

Wenn Sie einen Redshift-Cluster erstellen, sollten Sie den Standarddatenbanknamen in einen eindeutigen Wert ändern. Standardnamen sind allgemein bekannt und sollten bei der Konfiguration geändert werden. Beispielsweise könnte ein bekannter Name zu unbeabsichtigtem Zugriff führen, wenn er in IAM-Richtlinienbedingungen verwendet wird.

Abhilfe

Sie können den Datenbanknamen für Ihren Amazon Redshift Redshift-Cluster nicht ändern, nachdem er erstellt wurde. Anweisungen zum Erstellen eines neuen Clusters finden Sie unter [Erste Schritte mit Amazon Redshift](#) im Amazon Redshift Getting Started Guide.

[Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-2 NIST.800-53.R5 SI-7 (6)

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: AWS::Redshift::Cluster

AWS Config -Regel: [redshift-cluster-kms-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Amazon Redshift Redshift-Cluster im Ruhezustand verschlüsselt sind. Die Steuerung schlägt fehl, wenn ein Redshift-Cluster im Ruhezustand nicht verschlüsselt ist oder wenn sich der Verschlüsselungsschlüssel von dem im Regelparameter angegebenen Schlüssel unterscheidet.

In Amazon Redshift können Sie die Datenbankverschlüsselung für Ihre Cluster aktivieren, um Data-at-Rest besser zu schützen. Wenn Sie die Verschlüsselung für einen Cluster aktivieren, werden

die Datenblöcke und die Metadaten des Systems für den Cluster und Snapshots des Clusters verschlüsselt. Die Verschlüsselung ruhender Daten ist eine empfohlene bewährte Methode, da sie Ihren Daten eine Ebene der Zugriffsverwaltung hinzufügt. Durch die Verschlüsselung von Redshift-Clustern im Ruhezustand wird das Risiko verringert, dass ein nicht autorisierter Benutzer auf die auf der Festplatte gespeicherten Daten zugreifen kann.

Abhilfe

Informationen zur Änderung eines Redshift-Clusters für die Verwendung der KMS-Verschlüsselung finden Sie unter [Ändern der Cluster-Verschlüsselung](#) im Amazon Redshift Management Guide.

[Redshift.11] Redshift-Cluster sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Redshift::Cluster`

AWS Config Regel: `tagged-redshift-cluster` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplanytyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob ein Amazon Redshift Redshift-Cluster Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn der Cluster keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter `requiredTagKeys`

angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Cluster mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `aws:` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der [Allgemeine AWS-Referenz](#).

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Redshift-Cluster finden Sie unter [Tagging resources in Amazon Redshift](#) im Amazon Redshift Management Guide.

[Redshift.12] Abonnements für Redshift-Ereignisbenachrichtigungen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Redshift::EventSubscription`

AWS Config Regel: tagged-redshift-eventssubscription (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob ein Amazon Redshift Redshift-Cluster-Snapshot Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn der Cluster-Snapshot keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Cluster-Snapshot mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen

möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Abonnement für Redshift-Ereignisbenachrichtigungen finden Sie unter [Tagging resources in Amazon Redshift](#) im Amazon Redshift Management Guide.

[Redshift.13] Redshift-Cluster-Snapshots sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Redshift::ClusterSnapshot`

AWS Config Regel: `tagged-redshift-clustersnapshot` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS	No default value

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen.	

Dieses Steuerelement prüft, ob ein Amazon Redshift Redshift-Cluster-Snapshot Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn der Cluster-Snapshot keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Cluster-Snapshot mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der [Allgemeine AWS-Referenz](#).

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Redshift-Cluster-Snapshot finden Sie unter [Tagging resources in Amazon Redshift](#) im Amazon Redshift Management Guide.

[Redshift.14] Redshift-Cluster-Subnetzgruppen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Redshift::ClusterSubnetGroup`

AWS Config Regel: `tagged-redshift-cluster-subnetgroup` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob eine Amazon Redshift Redshift-Cluster-Subnetzgruppe Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind. `requiredTagKeys` Die Steuerung schlägt fehl, wenn die Cluster-Subnetzgruppe keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat. `requiredTagKeys` Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Cluster-Subnetzgruppe mit keinem Schlüssel

gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Redshift-Cluster-Subnetzgruppe finden Sie unter [Tagging resources in Amazon Redshift](#) im Amazon Redshift Management Guide.

[Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen

Verwandte Anforderungen: PCI DSS v4.0.1/1.3.1

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Sicherheitsgruppenkonfiguration

Schweregrad: Hoch

Art der Ressource: `AWS::Redshift::Cluster`

AWS Config -Regel: [redshift-unrestricted-port-access](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob eine mit einem Amazon Redshift Redshift-Cluster verknüpfte Sicherheitsgruppe über Eingangsregeln verfügt, die den Zugriff auf den Cluster-Port vom Internet aus ermöglichen (0.0.0.0/0 oder: :/0). Die Kontrolle schlägt fehl, wenn die Eingangsregeln der Sicherheitsgruppe den Zugriff auf den Cluster-Port über das Internet zulassen.

Das Zulassen eines uneingeschränkten eingehenden Zugriffs auf den Redshift-Cluster-Port (IP-Adresse mit dem Suffix /0) kann zu unbefugtem Zugriff oder Sicherheitsvorfällen führen. Wir empfehlen, bei der Erstellung von Sicherheitsgruppen und der Konfiguration von Regeln für eingehenden Datenverkehr das Prinzip des Zugriffs mit den geringsten Rechten anzuwenden.

Abhilfe

Informationen zur Beschränkung des Eingangs auf dem Redshift-Cluster-Port auf eingeschränkte Ursprünge finden Sie unter [Arbeiten mit Sicherheitsgruppenregeln](#) im Amazon VPC-Benutzerhandbuch. Aktualisieren Sie Regeln, bei denen der Portbereich mit dem Redshift-Cluster-Port übereinstimmt und der IP-Portbereich 0.0.0.0/0 ist.

[Redshift.16] Redshift-Cluster-Subnetzgruppen sollten Subnetze aus mehreren Availability Zones haben

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: AWS::Redshift::ClusterSubnetGroup

AWS Config -Regel: [redshift-cluster-subnet-group-multi-az](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Die Steuerung prüft, ob eine Amazon Redshift Redshift-Cluster-Subnetzgruppe Subnetze aus mehr als einer Availability Zone (AZ) hat. Die Steuerung schlägt fehl, wenn die Cluster-Subnetzgruppe keine Subnetze aus mindestens zwei verschiedenen Subnetzen hat. AZs

Durch die Konfiguration mehrerer AZs Subnetze wird sichergestellt, dass Ihr Redshift Data Warehouse auch bei Ausfällen weiterbetrieben werden kann.

Abhilfe

Informationen zum Ändern einer Redshift-Cluster-Subnetzgruppe, sodass sie sich über mehrere erstreckt AZs, finden Sie unter [Ändern einer Cluster-Subnetzgruppe](#) im Amazon Redshift Management Guide.

[Redshift.17] Redshift-Cluster-Parametergruppen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Redshift::ClusterParameterGroup`

AWS Config -Regel: [redshift-cluster-parameter-group-tagged](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Eine Liste der Tag-Schlüssel vom Typ „“, die einer ausgewerteten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon Redshift Redshift-Cluster-Parametergruppe die durch den `requiredKeyTags` Parameter angegebenen Tag-Schlüssel hat. Die Steuerung schlägt fehl, wenn die Parametergruppe keine Tag-Schlüssel oder nicht alle durch den `requiredKeyTags`

Parameter angegebenen Schlüssel hat. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Parametergruppe keine Tagschlüssel hat. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws :` Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im [Tagging AWS Resources and Tag](#) Editor User Guide.

 Note

Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Amazon Redshift-Cluster-Parametergruppe finden Sie unter [Tag-Ressourcen in Amazon Redshift](#) im Amazon Redshift Management Guide.

[Redshift.18] Für Redshift-Cluster sollten Multi-AZ-Bereitstellungen aktiviert sein

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::Redshift::Cluster`

AWS Config -Regel: [redshift-cluster-multi-az-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob mehrere Availability Zones (Multi-AZ) -Bereitstellungen für einen Amazon Redshift Redshift-Cluster aktiviert sind. Die Steuerung schlägt fehl, wenn Multi-AZ-Bereitstellungen für den Amazon Redshift Redshift-Cluster nicht aktiviert sind.

Amazon Redshift unterstützt mehrere Availability Zones (Multi-AZ) -Bereitstellungen für bereitgestellte Cluster. Wenn Multi-AZ-Bereitstellungen für einen Cluster aktiviert sind, kann ein Amazon Redshift Data Warehouse in Ausfallszenarien weiterarbeiten, wenn ein unerwartetes Ereignis in einer Availability Zone (AZ) eintritt. Eine Multi-AZ-Bereitstellung stellt Rechenressourcen in mehr als einer AZ bereit, und auf diese Rechenressourcen kann über einen einzigen Endpunkt zugegriffen werden. Im Falle eines vollständigen AZ-Ausfalls sind die verbleibenden Rechenressourcen in einer anderen AZ verfügbar, um die Verarbeitung von Workloads fortzusetzen. Sie können ein vorhandenes Single-AZ-Data Warehouse in ein Multi-AZ-Data Warehouse umwandeln. Zusätzliche Rechenressourcen werden dann in einer zweiten AZ bereitgestellt.

Abhilfe

Informationen zur Konfiguration von Multi-AZ-Bereitstellungen für einen Amazon Redshift-Cluster finden Sie unter [Konvertieren eines Single-AZ-Data Warehouse in ein Multi-AZ-Data Warehouse](#) im Amazon Redshift Management Guide.

Security Hub-Steuerelemente für Amazon Redshift Serverless

Diese AWS Security Hub Kontrollen bewerten den Service und die Ressourcen von Amazon Redshift Serverless. Die Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[RedshiftServerless.1] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen in VPC

Schweregrad: Hoch

Art der Ressource: `AWS::RedshiftServerless::Workgroup`

AWS Config -Regel: [redshift-serverless-workgroup-routes-within-vpc](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Mit diesem Steuerelement wird geprüft, ob Enhanced VPC Routing für eine Amazon-Redshift-Serverless-Arbeitsgruppe aktiviert ist. Die Steuerung schlägt fehl, wenn das erweiterte VPC-Routing für die Arbeitsgruppe deaktiviert ist.

Wenn Enhanced VPC Routing für eine Amazon-Redshift-Serverless-Arbeitsgruppe deaktiviert ist, leitet Amazon Redshift den Datenverkehr über das Internet weiter, einschließlich Datenverkehr an andere Services im -Netzwerk. AWS Wenn Sie Enhanced VPC Routing für eine Arbeitsgruppe aktivieren, erzwingt Amazon Redshift, dass der gesamte UNLOAD Datenverkehr zwischen Ihrem Cluster COPY und Ihren Datenrepositorys über Ihre Virtual Private Cloud (VPC) erfolgt, die auf dem Amazon-VPC-Service basiert. Mit Enhanced VPC Routing können Sie VPC-Standardfunktionen verwenden, um den Datenfluss zwischen Ihrem Amazon Redshift Redshift-Cluster und anderen Ressourcen zu steuern. Dazu gehören Funktionen wie VPC-Sicherheitsgruppen und Endpunktrichtlinien, Netzwerkzugriffskontrolllisten (ACLs) und DNS-Server (Domain Name System). Sie können auch VPC-Flow-Logs verwenden, um den UNLOAD Datenverkehr COPY zu überwachen.

Abhilfe

Weitere Informationen über erweitertes VPC-Routing und dessen Aktivierung für eine Arbeitsgruppe finden Sie unter [Steuern des Netzwerkverkehrs mit erweitertem Redshift-VPC-Routing im Amazon Redshift](#) Management Guide.

[RedshiftServerless.2] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: AWS::RedshiftServerless::Workgroup

AWS Config -Regel: [redshift-serverless-workgroup-encrypted-in-transit](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob Verbindungen zu einer Amazon Redshift Serverless-Arbeitsgruppe erforderlich sind, um Daten während der Übertragung zu verschlüsseln. Die Steuerung schlägt fehl, wenn der `require_ssl` Konfigurationsparameter für die Arbeitsgruppe auf `false` gesetzt ist.

Eine Amazon-Redshift-Serverless-Arbeitsgruppe ist eine Sammlung von Rechenressourcen, die Rechenressourcen wie RPU's VPC-Subnetzgruppen und Sicherheitsgruppen gruppiert. Zu den Eigenschaften einer Arbeitsgruppe gehören Netzwerk- und Sicherheitseinstellungen. Diese Einstellungen geben an, ob Verbindungen zu einer Arbeitsgruppe erforderlich sein sollen, um SSL zur Verschlüsselung von Daten während der Übertragung zu verwenden.

Abhilfe

Informationen zur Aktualisierung der Einstellungen für eine Amazon Redshift Serverless-Arbeitsgruppe, sodass SSL-Verbindungen erforderlich sind, finden Sie unter [Connecting to Amazon Redshift Serverless im Amazon Redshift Management Guide](#).

[RedshiftServerless.3] Serverlose Redshift-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Hoch

Art der Ressource: `AWS::RedshiftServerless::Workgroup`

AWS Config -Regel: [redshift-serverless-workgroup-no-public-access](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Mit diesem Steuerelement wird geprüft, ob der öffentliche Zugriff für eine Amazon-Redshift-Serverless-Arbeitsgruppe deaktiviert ist. Es bewertet die `publiclyAccessible` Eigenschaft einer Redshift Serverless-Arbeitsgruppe. Die Steuerung schlägt fehl, wenn der öffentliche Zugriff für die Arbeitsgruppe aktiviert ist (`true`).

Die Einstellung `public access (publiclyAccessible)` für eine Amazon-Redshift-Serverless-Arbeitsgruppe gibt an, ob über ein öffentliches Netzwerk auf die Arbeitsgruppe zugegriffen werden kann. Wenn der öffentliche Zugriff für eine Arbeitsgruppe aktiviert (`true`) ist, erstellt Amazon Redshift eine Elastic IP-Adresse, die die Arbeitsgruppe von außerhalb der VPC öffentlich zugänglich macht. Wenn Sie nicht möchten, dass eine Arbeitsgruppe öffentlich zugänglich ist, deaktivieren Sie den öffentlichen Zugriff für sie.

Abhilfe

Informationen zum Ändern der Einstellung für den öffentlichen Zugriff für eine Amazon Redshift Serverless-Arbeitsgruppe finden Sie unter [Anzeigen der Eigenschaften für eine Arbeitsgruppe](#) im Amazon Redshift Management Guide.

[RedshiftServerless.4] Serverlose Redshift-Namespaces sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys

Verwandte Anforderungen: NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), (10), 2 NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-7 (NIST.800-53.r5 SC-12), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-2 NIST.800-53.R5 SI-7 (6)

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: AWS::RedshiftServerless::Namespace

AWS Config -Regel: [redshift-serverless-namespaces-cmk-encryption](#)

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Zulässige Werte	Security Hub Hub-Standardwert
kmsKeyArns	Eine Liste von Amazon-Ressourcennamen (ARNs) AWS KMS keys , die in die Bewertung aufgenommen werden sollen. Das Steuerelement generiert	StringList (maximal 3 Elemente)	1—3 ARNs der vorhandenen KMS-Schlüssel. Beispiel: arn:aws:kms:us-west-2:11112223333:kms:key/1234abcd-12ab-3	Kein Standardwert

Parameter	Beschreibung	Typ	Zulässige Werte	Security Hub Hub-Stand ardwert
	einen FAILED Befund, wenn ein Redshift Serverless-Namespace nicht mit einem KMS-Schlüssel in der Liste verschlüsselt ist.		4cd-56ef-1234567890ab .	

Diese Kontrolle prüft, ob ein Amazon-Redshift-Serverless-Namespace verschlüsselt ist, wenn ein Kunde verwaltet wird. AWS KMS key Die Steuerung schlägt fehl, wenn der Redshift Serverless-Namespace nicht mit einem vom Kunden verwalteten KMS-Schlüssel verschlüsselt ist. Sie können optional eine Liste von KMS-Schlüsseln angeben, die das Steuerelement in die Bewertung einbeziehen soll.

In Amazon Redshift Serverless definiert ein Namespace einen logischen Container für Datenbankobjekte. Dieses Steuerelement überprüft regelmäßig, ob die Verschlüsselungseinstellungen für einen Namespace einen vom Kunden verwalteten AWS KMS key anstelle eines AWS verwalteten KMS-Schlüssels für die Verschlüsselung von Daten im Namespace angeben. Mit einem vom Kunden verwalteten KMS-Schlüssel haben Sie die volle Kontrolle über den Schlüssel. Dazu gehören die Definition und Pflege der Schlüsselrichtlinie, die Verwaltung von Zuschüssen, die Rotation von kryptografischem Material, die Zuweisung von Tags, die Erstellung von Aliasnamen sowie die Aktivierung und Deaktivierung des Schlüssels.

Abhilfe

Informationen zur Aktualisierung der Verschlüsselungseinstellungen für einen Amazon Redshift Serverless-Namespace und zur Angabe eines vom Kunden verwalteten AWS KMS key Namespace finden Sie unter [Ändern des AWS KMS key für einen Namespace](#) im Amazon Redshift Management Guide.

[RedshiftServerless.5] Redshift Serverless-Namespace sollten nicht den Standard-Admin-Benutzernamen verwenden

Kategorie: Identifizieren > Ressourcenkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::RedshiftServerless::Namespace`

AWS Config -Regel: [redshift-serverless-default-admin-check](#)

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Zulässige Werte	Security Hub Hub-Standardwert
<code>validAdminUserNames</code>	Eine Liste von Admin-Benutzernamen, die Redshift Serverless-Namespace verwenden sollten. Das Steuerelement generiert eine FAILED Feststellung, ob ein Namespace einen Admin-Benutzernamen verwendet, der nicht in der Liste enthalten ist. In der Liste kann	StringList (maximal 6 Artikel)	1—6 gültige Admin-Benutzernamen für Redshift Serverless-Namespace.	Kein Standardwert

Parameter	Beschreibung	Typ	Zulässige Werte	Security Hub Hub-Stand ardwert
	der Standardwert nicht angegeben werden,admin.			

Dieses Steuerelement prüft, ob der Admin-Benutzername für einen Amazon Redshift Serverless-Namespace der Standard-Admin-Benutzername ist. `admin` Die Steuerung schlägt fehl, wenn der Admin-Benutzername für den Redshift Serverless-Namespace lautet. `admin` Sie können optional eine Liste von Admin-Benutzernamen angeben, die das Steuerelement in die Bewertung einbeziehen soll.

Wenn Sie einen Amazon Redshift Serverless-Namespace erstellen, sollten Sie einen benutzerdefinierten Admin-Benutzernamen für den Namespace angeben. Der standardmäßige Admin-Benutzername ist `public knowledge`. Durch die Angabe eines benutzerdefinierten Admin-Benutzernamens können Sie beispielsweise dazu beitragen, das Risiko oder die Effektivität von Brute-Force-Angriffen gegen den Namespace zu verringern.

Abhilfe

Sie können den Admin-Benutzernamen für einen Amazon Redshift Serverless-Namespace mithilfe der Amazon Redshift Serverless-Konsole oder API ändern. Um ihn mithilfe der Konsole zu ändern, wählen Sie die Namespace-Konfiguration und wählen Sie dann im Menü Aktionen die Option [Administratoranmeldedaten bearbeiten](#) aus. [Um ihn programmgesteuert zu ändern, verwenden Sie den `UpdateNamespaceVorgang` oder, falls Sie den verwenden AWS CLI, führen Sie den Befehl `update-namespace` aus.](#) Wenn Sie den Admin-Benutzernamen ändern, müssen Sie gleichzeitig auch das Admin-Passwort ändern.

[RedshiftServerless.6] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Ressourcentyp: `AWS::RedshiftServerless::Namespace`

AWS Config -Regel: [redshift-serverless-publish-logs-to-cloudwatch](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon Redshift Serverless Namespace so konfiguriert ist, dass er Verbindungs- und Benutzerprotokolle nach Amazon Logs exportiert. CloudWatch Die Steuerung schlägt fehl, wenn der Redshift Serverless-Namespace nicht für den Export der Protokolle in Logs konfiguriert ist. CloudWatch

Wenn Sie Amazon Redshift Serverless so konfigurieren, dass Verbindungsprotokoll- (connectionlog) und Benutzerprotokolldaten (userlog) in eine Protokollgruppe in Amazon CloudWatch Logs exportiert werden, können Sie Ihre Protokolldatensätze sammeln und in einem dauerhaften Speicher speichern, der Sicherheits-, Zugriffs- und Verfügbarkeitsprüfungen und Audits unterstützt. Mit CloudWatch Logs können Sie auch Echtzeitanalysen von Protokolldaten durchführen und verwenden, CloudWatch um Alarme und Metriken zu erstellen.

Abhilfe

Um Protokolldaten für einen Amazon-Redshift-Serverless-Namespace zu exportieren, müssen die entsprechenden CloudWatch Protokolle für den Export in den Auditprotokollierungskonfigurationseinstellungen für den Namespace ausgewählt werden. Informationen zur Aktualisierung dieser Einstellungen finden Sie unter [Sicherheit und Verschlüsselung bearbeiten](#) im Amazon Redshift Management Guide.

[RedshiftServerless.7] Redshift Serverless-Namespace sollten nicht den Standard-Datenbanknamen verwenden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Identifizieren > Ressourcenkonfiguration

Schweregrad: Mittel

Art der Ressource: AWS::RedshiftServerless::Namespace

AWS Config -Regel: [redshift-serverless-default-db-name-check](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon Redshift Serverless-Namespace den Standarddatenbanknamen verwendet. Die Steuerung schlägt fehl, wenn der Redshift Serverless-Namespace den Standarddatenbanknamen verwendet.

Wenn Sie einen Amazon Redshift Serverless-Namespace erstellen, sollten Sie einen eindeutigen, benutzerdefinierten Wert für den Datenbanknamen angeben und nicht den Standarddatenbanknamen verwenden, der `public knowledge` lautet. Durch die Angabe eines anderen Datenbanknamens können Sie das Risiko verringern, dass nicht autorisierte Benutzer versehentlich auf Daten im Namespace zugreifen können.

Abhilfe

Sie können den Datenbanknamen für einen Amazon-Redshift-Serverless-Namespace nicht mehr ändern, nachdem Sie den Namespace erstellt haben. Sie können jedoch einen benutzerdefinierten Datenbanknamen für einen Redshift Serverless-Namespace angeben, wenn Sie den Namespace erstellen. Informationen zum Erstellen eines Namespaces finden Sie unter [Arbeitsgruppen und Namespaces](#) im Amazon Redshift Management Guide.

Security Hub-Steuerelemente für Route 53

Diese AWS Security Hub Kontrollen bewerten den Service und die Ressourcen von Amazon Route 53.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Route53::HealthCheck`

AWS Config Regel: `tagged-route53-healthcheck` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon Route 53-Zustandsprüfung Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind `requiredTagKeys`. Die Kontrolle schlägt fehl, wenn die Zustandsprüfung keine Tag-Schlüssel enthält oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Zustandsprüfung mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Stichwörtern zu einer Route 53-Zustandsprüfung finden Sie unter [Benennen und Kennzeichnen von Zustandsprüfungen](#) im Amazon Route 53-Entwicklerhandbuch.

[Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 (9), NIST.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8), PCI DSS v4.0.1/10.4.2

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS::Route53::HostedZone

AWS Config -Regel: [route53-query-logging-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die DNS-Abfrageprotokollierung für eine öffentlich gehostete Zone von Amazon Route 53 aktiviert ist. Die Steuerung schlägt fehl, wenn die DNS-Abfrageprotokollierung für eine öffentlich gehostete Route 53-Zone nicht aktiviert ist.

Das Protokollieren von DNS-Abfragen für eine von Route 53 gehostete Zone entspricht den DNS-Sicherheits- und Compliance-Anforderungen und sorgt für Transparenz. Die Protokolle enthalten Informationen wie die abgefragte Domäne oder Subdomäne, Datum und Uhrzeit der Abfrage, den

DNS-Eintragstyp (z. B. A oder AAAA) und den DNS-Antwortcode (z. B. `NoError` `ServFail`). Wenn die DNS-Abfrageprotokollierung aktiviert ist, veröffentlicht Route 53 die Protokolldateien in Amazon CloudWatch Logs.

Abhilfe

Informationen zum Protokollieren von DNS-Abfragen für öffentlich gehostete Route 53-Zonen finden Sie unter [Konfiguration der Protokollierung für DNS-Abfragen](#) im Amazon Route 53-Entwicklerhandbuch.

Security Hub-Steuerelemente für Amazon S3

Diese AWS Security Hub Kontrollen bewerten den Service und die Ressourcen des Amazon Simple Storage Service (Amazon S3). Die Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[S3.1] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/2.1.4, CIS AWS Foundations Benchmark v1.4.0/2.1.5, NIST.800-53.r5 AC-2 1,, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-3, (21), (11) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (16) NIST.800-53.r5 AC-6, (20) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.2.1, NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, PCI DSS v4.0.1/1.4.4 NIST.800-53.r5 SC-7

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: AWS:::Account

AWS Config -Regel: [s3-account-level-public-access-blocks-periodic](#)

Art des Zeitplans: Periodisch

Parameter:

- `ignorePublicAcls: true` (nicht anpassbar)

- `blockPublicPolicy`: `true` (nicht anpassbar)
- `blockPublicAcls`: `true` (nicht anpassbar)
- `restrictPublicBuckets`: `true` (nicht anpassbar)

Diese Kontrolle prüft, ob die oben genannten Amazon S3 S3-Einstellungen für den öffentlichen Zugriff blockieren auf Kontoebene für einen S3-Allzweck-Bucket konfiguriert sind. Die Steuerung schlägt fehl, wenn eine oder mehrere der Einstellungen zum Blockieren des öffentlichen Zugriffs auf gesetzt sind `false`.

Die Steuerung schlägt fehl `false`, wenn eine der Einstellungen auf eingestellt ist oder wenn eine der Einstellungen nicht konfiguriert ist.

Amazon S3 Public Access Block wurde entwickelt, um Kontrollen auf der gesamten AWS-Konto oder auf der Ebene einzelner S3-Buckets bereitzustellen, um sicherzustellen, dass Objekte niemals öffentlich zugänglich sind. Öffentlicher Zugriff auf Buckets und Objekte wird über Zugriffskontrolllisten (ACLs), Bucket-Richtlinien oder beides gewährt.

Sofern Sie nicht beabsichtigen, Ihre S3-Buckets öffentlich zugänglich zu machen, sollten Sie die Amazon S3 Block Public Access-Funktion auf Kontoebene konfigurieren.

Weitere Informationen finden Sie unter [Verwenden von Amazon S3 Block Public Access](#) im Amazon Simple Storage Service-Benutzerhandbuch.

Abhilfe

Informationen zur Aktivierung von Amazon S3 Block Public Access für Sie AWS-Konto finden Sie unter [Konfiguration der Einstellungen für den Block Public Access für Ihr Konto](#) im Amazon Simple Storage Service-Benutzerhandbuch.

[S3.2] S3-Allzweck-Buckets sollten den öffentlichen Lesezugriff blockieren

Verwandte Anforderungen: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.6, PCI DSS v3.2.1/7.2.1, NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7), (21), NIST.800-53.r5 AC-3, (11), (16) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (20) NIST.800-53.r5 AC-6, (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Kritisch

Art der Ressource: AWS::S3::Bucket

AWS Config -Regel: [s3-bucket-public-read-prohibited](#)

Art des Zeitplans: Periodisch und durch Änderung ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon S3 S3-Allzweck-Bucket öffentlichen Lesezugriff gewährt. Es überprüft die Einstellungen für „Block Public Access“ (Blockieren des öffentlichen Zugriffs), die Bucket-Richtlinie und die Bucket-Zugriffskontrollliste (ACL). Die Kontrolle schlägt fehl, wenn der Bucket öffentlichen Lesezugriff gewährt.

 Note

Wenn ein S3-Bucket über eine Bucket-Richtlinie verfügt, wertet dieses Steuerelement keine Richtlinienbedingungen aus, die Platzhalterzeichen oder Variablen verwenden. Um ein PASSED Ergebnis zu erzielen, dürfen Bedingungen in der Bucket-Richtlinie nur feste Werte verwenden, d. h. Werte, die keine Platzhalterzeichen oder Richtlinienvariablen enthalten. Informationen zu Richtlinienvariablen finden Sie unter [Variablen und Tags](#) im AWS Identity and Access Management Benutzerhandbuch.

In einigen Anwendungsfällen kann es erforderlich sein, dass jeder im Internet aus Ihrem S3-Bucket lesen kann. Solche Situationen sind jedoch selten. Um die Integrität und Sicherheit Ihrer Daten zu gewährleisten, sollte Ihr S3-Bucket nicht öffentlich lesbar sein.

Abhilfe

Informationen zum Blockieren des öffentlichen Lesezugriffs auf Ihre Amazon S3 S3-Buckets finden Sie unter [Konfiguration der Einstellungen zum Sperren des öffentlichen Zugriffs für Ihre S3-Buckets](#) im Amazon Simple Storage Service-Benutzerhandbuch.

[S3.3] S3-Allzweck-Buckets sollten den öffentlichen Schreibzugriff blockieren

Verwandte Anforderungen: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, PCI DSS v3.2.1/7.2.1, NIST.800-53.r5 AC-2 1,, NIST.800-53.r5 AC-3 (7), (21), (21), (11), (16) NIST.800-53.r5 AC-3, (20), NIST.800-53.r5 AC-4

(21) NIST.800-53.r5 AC-4, (3)) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Kritisch

Art der Ressource: AWS::S3::Bucket

AWS Config -Regel: [s3-bucket-public-write-prohibited](#)

Art des Zeitplans: Periodisch und durch Änderung ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon S3 S3-Allzweck-Bucket öffentlichen Schreibzugriff zulässt. Es überprüft die Einstellungen für „Block Public Access“ (Blockieren des öffentlichen Zugriffs), die Bucket-Richtlinie und die Bucket-Zugriffskontrollliste (ACL). Die Kontrolle schlägt fehl, wenn der Bucket öffentlichen Schreibzugriff zulässt.

Note

Wenn ein S3-Bucket über eine Bucket-Richtlinie verfügt, wertet dieses Steuerelement keine Richtlinienbedingungen aus, die Platzhalterzeichen oder Variablen verwenden. Um ein PASSED Ergebnis zu erzielen, dürfen Bedingungen in der Bucket-Richtlinie nur feste Werte verwenden, d. h. Werte, die keine Platzhalterzeichen oder Richtlinienvariablen enthalten. Informationen zu Richtlinienvariablen finden Sie unter [Variablen und Tags](#) im AWS Identity and Access Management Benutzerhandbuch.

Einige Anwendungsfälle erfordern, dass jeder im Internet in den S3-Bucket schreiben kann. Solche Situationen sind jedoch selten. Um die Integrität und Sicherheit Ihrer Daten zu gewährleisten, sollte Ihr S3-Bucket nicht öffentlich beschreibbar sein.

Abhilfe

Informationen zum Blockieren des öffentlichen Schreibzugriffs auf Ihre Amazon S3 S3-Buckets finden Sie unter [Konfiguration der Einstellungen zum Sperren des öffentlichen Zugriffs für Ihre S3-Buckets](#) im Amazon Simple Storage Service-Benutzerhandbuch.

[S3.5] S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erfordern

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/2.1.1, CIS AWS Foundations Benchmark v1.4.0/2.1.2, NIST.800-53.r5 AC-1 7 (2), (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 NIST.800-53.r5 IA-5 (3), 3, 3 (3), NIST.800-53.r5 SC-1 NIST.800-53.r5 SC-2 (4),, NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-7 (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.R5 SI-7 NIST.800-53.r5 SC-8 (6), NIST.800-171.r2 3.13.15, PCI DSS v3.2.1/4.1, PCI DSS v4.0.1/4.2.1

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: AWS::S3::Bucket

AWS Config -Regel: [s3-bucket-ssl-requests-only](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon S3 S3-Allzweck-Bucket über eine Richtlinie verfügt, die verlangt, dass Anfragen SSL verwenden. Die Kontrolle schlägt fehl, wenn die Bucket-Richtlinie keine Anfragen zur Verwendung von SSL erfordert.

S3-Buckets sollten über Richtlinien verfügen, die vorschreiben, dass alle Anfragen (Action: S3:*) in der S3-Ressourcenrichtlinie, wie durch den Bedingungsschlüssel `aws:SecureTransport` angegeben, nur die Übertragung von Daten über HTTPS akzeptieren.

Abhilfe

Informationen zur Aktualisierung einer Amazon S3 S3-Bucket-Richtlinie, um unsicheren Transport zu verweigern, finden Sie unter [Hinzufügen einer Bucket-Richtlinie mithilfe der Amazon S3 S3-Konsole](#) im Amazon Simple Storage Service-Benutzerhandbuch.

Fügen Sie eine Richtlinienerklärung hinzu, die der in der folgenden Richtlinie ähnelt. `amzn-s3-demo-bucket` Ersetzen Sie es durch den Namen des Buckets, den Sie ändern.

JSON

```
{
```

```

    "Id": "ExamplePolicy",
    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "AllowSSLRequestsOnly",
        "Action": "s3:*",
        "Effect": "Deny",
        "Resource": [
          "arn:aws:s3:::amzn-s3-demo-bucket",
          "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ],
        "Condition": {
          "Bool": {
            "aws:SecureTransport": "false"
          }
        },
        "Principal": "*"
      }
    ]
  }
}

```

Weitere Informationen finden Sie unter [Welche S3-Bucket-Richtlinie sollte ich verwenden, um die AWS Config Regel s3- einzuhaltenbucket-ssl-requests-only?](#) im AWS offiziellen Knowledge Center.

[S3.6] Allgemeine S3-Bucket-Richtlinien sollten den Zugriff auf andere einschränken AWS-Konten

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-171.r2 3.13.4

Kategorie: Schützen > Sichere Zugriffsverwaltung > Eingeschränkte Aktionen für sensible API-Operationen

Schweregrad: Hoch

Art der Ressource: AWS::S3::Bucket

AWS Config-Regel: [s3-bucket-blacklisted-actions-prohibited](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `blacklistedactionpatterns`: `s3:DeleteBucketPolicy`, `s3:PutBucketAcl`, `s3:PutBucketPolicy`, `s3:PutEncryptionConfiguration`, `s3:PutObjectAcl` (nicht anpassbar)

Diese Kontrolle prüft, ob eine allgemeine Amazon S3 S3-Bucket-Richtlinie verhindert, dass Principals AWS-Konten von anderen Personen abgelehnte Aktionen für Ressourcen im S3-Bucket ausführen. Die Kontrolle schlägt fehl, wenn die Bucket-Richtlinie eine oder mehrere der vorherigen Aktionen für einen Prinzipal in einem anderen AWS-Konto zulässt.

Die Implementierung des Zugriffs mit den geringsten Rechten ist von grundlegender Bedeutung, um das Sicherheitsrisiko und die Auswirkungen von Fehlern oder böswilligen Absichten zu verringern. Wenn eine S3-Bucket-Richtlinie den Zugriff von externen Konten aus ermöglicht, kann dies zu einer Datenexfiltration durch eine Insider-Bedrohung oder einen Angreifer führen.

Der `blacklistedactionpatterns` Parameter ermöglicht eine erfolgreiche Auswertung der Regel für S3-Buckets. Der Parameter gewährt Zugriff auf externe Konten für Aktionsmuster, die nicht in der `blacklistedactionpatterns` Liste enthalten sind.

Abhilfe

Informationen zum Aktualisieren einer Amazon S3 S3-Bucket-Richtlinie zum Entfernen von Berechtigungen finden Sie unter [Hinzufügen einer Bucket-Richtlinie mithilfe der Amazon S3 S3-Konsole](#) im Amazon Simple Storage Service-Benutzerhandbuch.

Führen Sie auf der Seite Bucket-Richtlinie bearbeiten im Textfeld zur Richtlinienbearbeitung eine der folgenden Aktionen aus:

- Entfernen Sie die Anweisungen, die anderen AWS-Konten Zugriff auf abgelehnte Aktionen gewähren.
- Entfernen Sie die zulässigen verweigerten Aktionen aus den Anweisungen.

[S3.7] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden

Verwandte Anforderungen: PCI DSS v3.2.1/2.2, NIST.800-53.r5 AU-9(2), NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-3 6 (2), (2), NIST.800-53.R5 SI-13 NIST.800-53.r5 SC-5 (5)

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Niedrig

Art der Ressource: AWS::S3::Bucket

AWS Config Regel: [s3-bucket-cross-region-replication-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für einen Amazon S3 S3-Allzweck-Bucket die regionsübergreifende Replikation aktiviert ist. Die Steuerung schlägt fehl, wenn für den Bucket keine regionsübergreifende Replikation aktiviert ist.

Bei der Replikation handelt es sich um das automatische, asynchrone Kopieren von Objekten zwischen Buckets, die sich im selben oder in unterschiedlichen Buckets befinden. AWS-Regionen Bei der Replikation werden neu erstellte Objekte und Objektaktualisierungen von einem Quell-Bucket in einen oder mehrere Ziel-Buckets kopiert. AWS In bewährten Verfahren wird die Replikation für Quell- und Ziel-Buckets empfohlen, die demselben Eigentümer gehören. AWS-Konto Zusätzlich zur Verfügbarkeit sollten Sie andere Einstellungen für die Systemstabilisierung berücksichtigen.

Dieses Steuerelement generiert einen FAILED Befund für einen Replizierungsziel-Bucket, wenn für diesen keine regionsübergreifende Replikation aktiviert ist. Wenn es einen legitimen Grund dafür gibt, dass für die Aktivierung des Ziel-Buckets keine regionsübergreifende Replikation erforderlich ist, können Sie die Ergebnisse für diesen Bucket unterdrücken.

Abhilfe

Informationen zur Aktivierung der regionsübergreifenden Replikation auf einem S3-Bucket finden Sie unter [Konfiguration der Replikation für Quell- und Ziel-Buckets, die demselben Konto gehören](#), im Amazon Simple Storage Service-Benutzerhandbuch. Wählen Sie für Quell-Bucket die Option Auf alle Objekte im Bucket anwenden aus.

[S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/2.1.4, CIS AWS Foundations Benchmark v1.4.0/2.1.5, NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-3, (21), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (11), (16) NIST.800-53.r5 AC-6, (20) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v4.0.1/1.4.4 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Kategorie: Schützen > Sicheres Zugriffsmanagement > Zugriffskontrolle

Schweregrad: Hoch

Art der Ressource: AWS::S3::Bucket

AWS Config -Regel: [s3-bucket-level-public-access-prohibited](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `excludedPublicBuckets`(nicht anpassbar) — Eine durch Kommas getrennte Liste bekannter zulässiger öffentlicher S3-Bucket-Namen

Diese Kontrolle prüft, ob ein Amazon S3 S3-Allzweck-Bucket den öffentlichen Zugriff auf Bucket-Ebene blockiert. Die Steuerung schlägt fehl, wenn eine der folgenden Einstellungen auf `false` ist:

- `ignorePublicAcls`
- `blockPublicPolicy`
- `blockPublicAcls`
- `restrictPublicBuckets`

Block Public Access auf S3-Bucket-Ebene bietet Kontrollen, mit denen sichergestellt wird, dass Objekte niemals öffentlich zugänglich sind. Öffentlicher Zugriff auf Buckets und Objekte wird über Zugriffskontrolllisten (ACLs), Bucket-Richtlinien oder beides gewährt.

Sofern Sie nicht beabsichtigen, Ihre S3-Buckets öffentlich zugänglich zu machen, sollten Sie die Amazon S3 Block Public Access-Funktion auf Bucket-Ebene konfigurieren.

Abhilfe

Informationen zum Entfernen des öffentlichen Zugriffs auf Bucket-Ebene finden Sie unter [Blockieren des öffentlichen Zugriffs auf Ihren Amazon S3 S3-Speicher](#) im Amazon S3 S3-Benutzerhandbuch.

[S3.9] Bei S3-Allzweck-Buckets sollte die Serverzugriffsprotokollierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5

AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-3
NIST.800-53.r5 SC-7 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8), NIST.800-171.R2
3.3.8, PCI DSS v4.0.1/10.2.1

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Ressourcentyp: AWS::S3::Bucket

AWS Config -Regel: [s3-bucket-logging-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Serverzugriffsprotokollierung für einen Amazon S3 S3-Allzweck-Bucket aktiviert ist. Die Steuerung schlägt fehl, wenn die Serverzugriffsprotokollierung nicht aktiviert ist. Wenn die Protokollierung aktiviert ist, übermittelt Amazon S3 Zugriffsprotokolle für einen Quell-Bucket an einen ausgewählten Ziel-Bucket. Der Ziel-Bucket muss sich in der selben AWS-Region wie der Quell-Bucket befinden und es darf kein standardmäßiger Aufbewahrungszeitraum konfiguriert sein. Für den Ziel-Logging-Bucket muss die Serverzugriffsprotokollierung nicht aktiviert sein, und Sie sollten die Ergebnisse für diesen Bucket unterdrücken.

Die Serverzugriffsprotokollierung bietet detaillierte Aufzeichnungen der Anfragen, die an einen Bucket gestellt wurden. Serverzugriffsprotokolle können bei Sicherheits- und Zugriffsprüfungen hilfreich sein. Weitere Informationen finden Sie unter [Bewährte Sicherheitsmethoden für Amazon S3: Aktivieren Sie die Amazon S3 S3-Serverzugriffsprotokollierung](#).

Abhilfe

Informationen zur Aktivierung der Amazon S3 S3-Serverzugriffsprotokollierung finden Sie unter [Aktivieren der Amazon S3 S3-Serverzugriffsprotokollierung](#) im Amazon S3 S3-Benutzerhandbuch.

[S3.10] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS::S3::Bucket

AWS Config -Regel: [s3-version-lifecycle-policy-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein versionsbasierter Amazon S3 S3-Bucket für allgemeine Zwecke über eine Lifecycle-Konfiguration verfügt. Die Kontrolle schlägt fehl, wenn der Bucket keine Lifecycle-Konfiguration hat.

Wir empfehlen, eine Lifecycle-Konfiguration für Ihren S3-Bucket zu erstellen, um Ihnen bei der Definition von Aktionen zu helfen, die Amazon S3 während der Lebensdauer eines Objekts ausführen soll.

Abhilfe

Weitere Informationen zur Konfiguration des Lebenszyklus in einem Amazon S3 S3-Bucket finden Sie unter [Lebenszykluskonfiguration für einen Bucket einrichten](#) und [Ihren Speicherlebenszyklus verwalten](#).

[S3.11] Bei S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-3 (8), NIST.800-53.R5 SI-4, NIST.800-53.R5 SI-4 (4), NIST.800-171.R2 3.3.8

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS::S3::Bucket

AWS Config -Regel: [s3-event-notifications-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
eventTypes	Liste der bevorzugten S3-Ereignistypen	EnumList (maximal 28 Artikel)	s3:IntelligentTiering, s3:LifecycleExpiration:*, s3:LifecycleExpiration:Delete, s3:LifecycleExpiration:DeleteMarkerCreated, s3:LifecycleTransition, s3:ObjectAcl:Put, s3:ObjectCreated:*, , s3:ObjectCreated:CompleteMultipartUpload, s3:ObjectCreated:Copy,	Kein Standardwert

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
			s3:ObjectCreated:Post, s3:ObjectCreated:Put, s3:ObjectRemoved:* , s3:ObjectRemoved:Delete, s3:ObjectRemoved:DeleteMarkerCreated , s3:ObjectRestore:* , s3:ObjectRestore:Completed, s3:ObjectRestore:Delete, s3:ObjectRestore:Post, s3:ObjectTagging:* ,	

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
			s3:ObjectTagging:Delete, s3:ObjectTagging:Put, s3:ReducedRedundancyLostObject, s3:Replication:*, s3:Replication:OperationFailedReplication, s3:Replication:OperationMissedThreshold, s3:Replication:OperationNotTracked, s3:Replication:OperationReplicatedAfterThreshold,	

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert

s3:TestEvent

Dieses Steuerelement prüft, ob S3-Ereignisbenachrichtigungen in einem Amazon S3 S3-Allzweck-Bucket aktiviert sind. Die Steuerung schlägt fehl, wenn S3-Ereignisbenachrichtigungen für den Bucket nicht aktiviert sind. Wenn Sie benutzerdefinierte Werte für den eventTypes Parameter angeben, wird die Steuerung nur erfolgreich ausgeführt, wenn Ereignisbenachrichtigungen für die angegebenen Ereignistypen aktiviert sind.

Wenn Sie S3-Ereignisbenachrichtigungen aktivieren, erhalten Sie Benachrichtigungen, wenn bestimmte Ereignisse eintreten, die sich auf Ihre S3-Buckets auswirken. Sie können beispielsweise über die Erstellung, Entfernung von Objekten und Wiederherstellung von Objekten informiert werden. Diese Benachrichtigungen können die zuständigen Teams vor versehentlichen oder vorsätzlichen Änderungen warnen, die zu unberechtigtem Datenzugriff führen können.

Abhilfe

Informationen zum Erkennen von Änderungen an S3-Buckets und Objekten finden Sie unter [Amazon S3 S3-Ereignisbenachrichtigungen](#) im Amazon S3 S3-Benutzerhandbuch.

[S3.12] ACLs sollte nicht zur Verwaltung des Benutzerzugriffs auf S3-Allzweck-Buckets verwendet werden

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15) NIST.800-53.r5 AC-3, (7), NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6

Kategorie: Schützen > Sicheres Zugriffsmanagement > Zugriffskontrolle

Schweregrad: Mittel

Art der Ressource: AWS::S3::Bucket

AWS Config -Regel: [s3-bucket-acl-prohibited](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon S3 S3-Allzweck-Bucket Benutzerberechtigungen mit einer Zugriffskontrollliste (ACL) bereitstellt. Die Kontrolle schlägt fehl, wenn eine ACL für die Verwaltung des Benutzerzugriffs auf den Bucket konfiguriert ist.

ACLs sind veraltete Zugriffskontrollmechanismen, die älter als IAM sind. Stattdessen empfehlen wir ACLs, S3-Bucket-Richtlinien oder AWS Identity and Access Management (IAM-) Richtlinien zu verwenden, um den Zugriff auf Ihre S3-Buckets zu verwalten.

Abhilfe

Um diese Kontrolle zu bestehen, sollten Sie die ACLs für Ihre S3-Buckets deaktivieren. Anweisungen finden Sie unter [Kontrolle des Besitzes von Objekten und Deaktivierung ACLs für Ihren Bucket](#) im Amazon Simple Storage Service-Benutzerhandbuch.

Informationen zum Erstellen einer S3-Bucket-Richtlinie finden Sie unter [Hinzufügen einer Bucket-Richtlinie mithilfe der Amazon S3 S3-Konsole](#). Informationen zum Erstellen einer IAM-Benutzerrichtlinie für einen S3-Bucket finden Sie unter [Steuern des Zugriffs auf einen Bucket mit Benutzerrichtlinien](#).

[S3.13] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Schützen > Datenschutz

Schweregrad: Niedrig

Art der Ressource: AWS::S3::Bucket

AWS Config -Regel: [s3-lifecycle-policy-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>targetTransitionDays</code>	Anzahl der Tage nach der Objekterstellung, an denen Objekte in eine angegebene Speicherklasse umgestellt werden	Ganzzahl	1 auf 36500	Kein Standardwert
<code>targetExpirationDays</code>	Anzahl der Tage nach der Objekterstellung, an denen Objekte gelöscht werden	Ganzzahl	1 auf 36500	Kein Standardwert
<code>targetTransitionStorageClasses</code>	Typ der S3-Speicherklasse des Ziels	Enum	STANDARD_IA, INTELLIGENT_TIERING, ONEZONE_IA, GLACIER, GLACIER_IR, DEEP_ARCHIVE	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon S3 S3-Allzweck-Bucket über eine Lifecycle-Konfiguration verfügt. Die Steuerung schlägt fehl, wenn der Bucket keine Lifecycle-Konfiguration hat. Wenn Sie benutzerdefinierte Werte für einen oder mehrere der oben genannten Parameter angeben, ist die Kontrolle nur erfolgreich, wenn die Richtlinie die angegebene Speicherklasse, Löschzeit oder Übergangszeit beinhaltet.

Durch das Erstellen einer Lifecycle-Konfiguration für Ihren S3-Bucket werden Aktionen definiert, die Amazon S3 während der Lebensdauer eines Objekts ausführen soll. Sie können beispielsweise

Objekte in eine andere Speicherkategorie übertragen, archivieren oder nach einem bestimmten Zeitraum löschen.

Abhilfe

Informationen zur Konfiguration von Lebenszyklusrichtlinien für einen Amazon S3 S3-Bucket finden Sie unter [Einstellung der Lebenszykluskonfiguration für einen Bucket](#) und unter [Verwaltung Ihres Speicherlebenszyklus](#) im Amazon S3 S3-Benutzerhandbuch.

[S3.14] Für S3-Allzweck-Buckets sollte die Versionierung aktiviert sein

Kategorie: Schützen > Datenschutz > Schutz vor Datenlöschung

Verwandte Anforderungen: NIST.800-53.r5 AU-9(2), NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-12, NIST.800-53.R5 SI-13 (5), NIST.800-171.R2 3.3.8

Schweregrad: Niedrig

Art der Ressource: AWS::S3::Bucket

AWS Config -Regel: [s3-bucket-versioning-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für einen Amazon S3 S3-Allzweck-Bucket die Versionierung aktiviert ist. Die Kontrolle schlägt fehl, wenn die Versionierung für den Bucket ausgesetzt ist.

Bei der Versionierung werden mehrere Varianten eines Objekts im selben S3-Bucket aufbewahrt. Sie können die Versionierung verwenden, um frühere Versionen eines in Ihrem S3-Bucket gespeicherten Objekts beizubehalten, abzurufen und wiederherzustellen. Die Versionierung hilft Ihnen bei der Wiederherstellung sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern.

Tip

Wenn die Anzahl der Objekte in einem Bucket aufgrund der Versionierung zunimmt, können Sie eine Lifecycle-Konfiguration einrichten, um versionierte Objekte auf der Grundlage von

Regeln automatisch zu archivieren oder zu löschen. Weitere Informationen finden Sie unter [Amazon S3 Lifecycle Management für versionierte Objekte](#).

Abhilfe

Informationen zur Verwendung der Versionierung in einem S3-Bucket finden Sie unter [Aktivieren der Versionierung für Buckets](#) im Amazon S3 S3-Benutzerhandbuch.

[S3.15] Bei S3-Allzweck-Buckets sollte Object Lock aktiviert sein

Kategorie: Schützen > Datenschutz > Schutz vor Datenlöschung

Verwandte Anforderungen: NIST.800-53.R5 CP-6 (2), PCI DSS v4.0.1/10.5.1

Schweregrad: Mittel

Art der Ressource: AWS::S3::Bucket

AWS Config -Regel: [s3-bucket-default-lock-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
mode	Aufbewahrungsmodus von S3 Object Lock	Enum	GOVERNANCE , COMPLIANCE	Kein Standardwert

Dieses Steuerelement prüft, ob in einem Amazon S3 S3-Allzweck-Bucket Object Lock aktiviert ist. Die Steuerung schlägt fehl, wenn Object Lock für den Bucket nicht aktiviert ist. Wenn Sie einen benutzerdefinierten Wert für den mode Parameter angeben, wird die Steuerung nur erfolgreich ausgeführt, wenn S3 Object Lock den angegebenen Aufbewahrungsmodus verwendet.

Sie können S3 Object Lock verwenden, um Objekte mithilfe eines write-once-read-many (WORM-) Modells zu speichern. Object Lock kann verhindern, dass Objekte in S3-Buckets für einen bestimmten Zeitraum oder auf unbestimmte Zeit gelöscht oder überschrieben werden. Sie können die S3-Objektsperre verwenden, um regulatorische Anforderungen einzuhalten, die die WORM-Speicherung verlangen, oder um eine zusätzliche Schutzebene gegen Objektänderungen und -löschungen einzurichten.

Abhilfe

Informationen zur Konfiguration von Object Lock für neue und bestehende S3-Buckets finden Sie unter [Konfiguration von S3 Object Lock](#) im Amazon S3 S3-Benutzerhandbuch.

[S3.17] S3-Allzweck-Buckets sollten im Ruhezustand verschlüsselt werden mit AWS KMS keys

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Verwandte Anforderungen: NIST.800-53.r5 SC-1 2 (2), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8 (1), (10), NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-7 NIST.800-53.R5 SI-7 NIST.800-53.r5 CA-9 (6), NIST.800-53.R5 AU-9, NIST.800-171.r2 3.8.9, NIST.800-171.r2 3.13.11, NIST.800-171.r2 3.13.16, PCI DSS v4.0.1/3.5.1

Schweregrad: Mittel

Art der Ressource: AWS::S3::Bucket

AWS Config -Regel: [s3-default-encryption-kms](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon S3 S3-Allzweck-Bucket mit einem AWS KMS key (SSE-KMS oder DSSE-KMS) verschlüsselt ist. Die Steuerung schlägt fehl, wenn der Bucket mit der Standardverschlüsselung (SSE-S3) verschlüsselt ist.

Serverseitige Verschlüsselung (SSE) ist die Verschlüsselung von Daten am Zielort durch die Anwendung oder den Dienst, der sie empfängt. Sofern Sie nichts anderes angeben, verwenden S3-Buckets standardmäßig Amazon S3 S3-verwaltete Schlüssel (SSE-S3) für die serverseitige Verschlüsselung. Für zusätzliche Kontrolle können Sie Buckets jedoch so konfigurieren, dass sie stattdessen serverseitige Verschlüsselung mit AWS KMS keys (SSE-KMS oder DSSE-KMS)

verwenden. Amazon S3 verschlüsselt Ihre Daten auf Objektebene, wenn es sie auf Festplatten in AWS Rechenzentren schreibt, und entschlüsselt sie für Sie, wenn Sie darauf zugreifen.

Abhilfe

Informationen zum Verschlüsseln eines S3-Buckets mit SSE-KMS finden Sie unter [Serverseitige Verschlüsselung mit AWS KMS \(SSE-KMS\) angeben](#) im Amazon S3 S3-Benutzerhandbuch.

Informationen zum Verschlüsseln eines S3-Buckets mit DSSE-KMS finden Sie unter [Spezifizierung der serverseitigen Dual-Layer-Verschlüsselung mit AWS KMS keys \(DSSE-KMS\)](#) im Amazon S3 S3-Benutzerhandbuch.

[S3.19] Bei S3-Zugriffspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v4.0.1/1.4.4

Kategorie: Schützen > Sichere Zugriffsverwaltung > Ressource nicht öffentlich zugänglich

Schweregrad: Kritisch

Art der Ressource: AWS::S3::AccessPoint

AWS Config -Regel: [s3-access-point-public-access-blocks](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob für einen Amazon S3 S3-Zugriffspunkt die Einstellungen für den öffentlichen Zugriff blockiert aktiviert sind. Die Kontrolle schlägt fehl, wenn die Einstellungen zum Blockieren des öffentlichen Zugriffs für den Access Point nicht aktiviert sind.

Die Amazon S3 S3-Funktion Block Public Access hilft Ihnen, den Zugriff auf Ihre S3-Ressourcen auf drei Ebenen zu verwalten: Konto-, Bucket- und Access Point-Ebene. Die Einstellungen auf jeder Ebene können unabhängig voneinander konfiguriert werden, sodass Sie unterschiedliche Stufen der öffentlichen Zugriffsbeschränkungen für Ihre Daten festlegen können. Die Einstellungen des Access Points können die restriktiveren Einstellungen auf höheren Ebenen (Kontoebene oder dem Access Point zugewiesener Bucket) nicht einzeln außer Kraft setzen. Stattdessen sind die Einstellungen

auf der Zugriffspunktebene additiv, was bedeutet, dass sie die Einstellungen auf den anderen Ebenen ergänzen und mit ihnen zusammenarbeiten. Sofern Sie nicht beabsichtigen, dass ein S3-Zugriffspunkt öffentlich zugänglich ist, sollten Sie die Einstellungen zum Blockieren des öffentlichen Zugriffs aktivieren.

Abhilfe

Amazon S3 unterstützt derzeit nicht das Ändern der Public Block Access-Einstellungen eines Zugriffspunkts, nachdem der Zugriffspunkt erstellt wurde. Alle Einstellungen zum Blockieren des öffentlichen Zugriffs sind standardmäßig aktiviert, wenn Sie einen neuen Access Point erstellen. Wir empfehlen, alle Einstellungen aktiviert zu lassen, es sei denn, Sie wissen, dass Sie eine bestimmte Einstellung deaktivieren müssen. Weitere Informationen finden Sie unter [Verwaltung des öffentlichen Zugriffs auf Access Points](#) im Amazon Simple Storage Service-Benutzerhandbuch.

[S3.20] Bei S3-Allzweck-Buckets sollte MFA Delete aktiviert sein

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/2.1.2, CIS AWS Foundations Benchmark v1.4.0/2.1.3, (1), (2) NIST.800-53.r5 CA-9 NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5

Kategorie: Schützen > Datenschutz > Schutz vor Datenlöschung

Schweregrad: Niedrig

Art der Ressource: AWS::S3::Bucket

AWS Config -Regel: [s3-bucket-mfa-delete-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob das Löschen mit Multi-Faktor-Authentifizierung (MFA) für einen Amazon S3 S3-Allzweck-Bucket aktiviert ist. Die Steuerung schlägt fehl, wenn MFA Delete für den Bucket nicht aktiviert ist. Das Steuerelement liefert keine Ergebnisse für Buckets mit einer Lebenszykluskonfiguration.

Wenn Sie die Versionierung für einen S3-Allzweck-Bucket aktivieren, können Sie optional eine weitere Sicherheitsebene hinzufügen, indem Sie MFA Delete für den Bucket konfigurieren. In diesem Fall muss der Bucket-Besitzer in jeder Anfrage zwei Arten der Authentifizierung angeben, um eine Version eines Objekts im Bucket zu löschen oder den Versionsstatus des Buckets zu ändern. MFA

Delete bietet zusätzliche Sicherheit, wenn beispielsweise die Sicherheitsanmeldedaten des Bucket-Besitzers kompromittiert wurden. Das Löschen mit MFA kann auch dazu beitragen, versehentliches Löschen von Buckets zu verhindern, indem der Benutzer, der die Löschaktion initiiert, den physischen Besitz eines MFA-Geräts mit einem MFA-Code nachweisen muss, wodurch die Löschaktion noch reibungsloser und sicherer wird.

 Note

Dieses Steuerelement erzeugt nur dann ein PASSED Ergebnis, wenn MFA Delete für den S3-Allzweck-Bucket aktiviert ist. Um MFA Delete für einen Bucket zu aktivieren, muss die Versionierung auch für den Bucket aktiviert sein. Die Bucket-Versionierung ist eine Methode zum Speichern mehrerer Varianten eines S3-Objekts im selben Bucket. Darüber hinaus kann nur der Bucket-Besitzer, der als Root-Benutzer angemeldet ist, das Löschen von MFA aktivieren und Löschaktionen für den Bucket ausführen. Sie können MFA Delete nicht mit einem Bucket verwenden, der über eine Lebenszykluskonfiguration verfügt.

Abhilfe

Informationen zur Aktivierung der Versionierung und zur Konfiguration von MFA Delete für einen S3-Bucket finden Sie unter [MFA-Löschen konfigurieren](#) im Amazon Simple Storage Service-Benutzerhandbuch.

[S3.22] S3-Allzweck-Buckets sollten Schreibereignisse auf Objektebene protokollieren

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/3.8, PCI DSS v4.0.1/10.2.1

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS : : : Account

AWS Config -Regel: [cloudtrail-all-write-s3-data-event-check](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein AWS-Konto über mindestens einen AWS CloudTrail Multiregions-Trail verfügt, der alle Schreibdatenereignisse für Amazon S3 S3-Buckets protokolliert. Die Kontrolle

schlägt fehl, wenn das Konto nicht über einen Multi-Regions-Trail verfügt, der Schreibdatenereignisse für S3-Buckets protokolliert.

S3-Operationen auf Objektebene, wie, und `GetObject DeleteObjectPutObject`, werden als Datenereignisse bezeichnet. Standardmäßig protokolliert CloudTrail es keine Datenereignisse, aber Sie können Trails konfigurieren, um Datenereignisse für S3-Buckets zu protokollieren. Wenn Sie die Protokollierung auf Objektebene für Schreibdatenereignisse aktivieren, können Sie jeden einzelnen Objekt- (Datei-) Zugriff innerhalb eines S3-Buckets protokollieren. Durch die Aktivierung der Protokollierung auf Objektebene können Sie mithilfe von Amazon Events Datenkonformitätsanforderungen erfüllen, umfassende Sicherheitsanalysen durchführen AWS-Konto, bestimmte Muster des Benutzerverhaltens in Ihrem System überwachen und Maßnahmen gegen API-Aktivitäten auf Objektebene innerhalb Ihrer S3-Buckets ergreifen. CloudWatch Diese Steuerung führt zu Ergebnissen, wenn Sie PASSED einen Trail mit mehreren Regionen konfigurieren, der nur Schreibvorgänge oder alle Arten von Datenereignissen für alle S3-Buckets protokolliert.

Abhilfe

Informationen zum Aktivieren der Protokollierung auf Objektebene für S3-Buckets finden Sie unter [Aktivieren der CloudTrail Ereignisprotokollierung für S3-Buckets und Objekte](#) im Amazon Simple Storage Service-Benutzerhandbuch.

[S3.23] S3-Allzweck-Buckets sollten Leseereignisse auf Objektebene protokollieren

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/3.9, PCI DSS v4.0.1/10.2.1

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS :: Account

AWS Config -Regel: [cloudtrail-all-read-s3-data-event-check](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein AWS-Konto über mindestens einen AWS CloudTrail Multiregions-Trail verfügt, der alle Lesedatenereignisse für Amazon S3 S3-Buckets protokolliert. Die Kontrolle schlägt fehl, wenn das Konto nicht über einen Multi-Regions-Trail verfügt, der Lesedatenereignisse für S3-Buckets protokolliert.

S3-Operationen auf Objektebene, wie, und `GetObject` `DeleteObject` `PutObject`, werden als Datenereignisse bezeichnet. Standardmäßig protokolliert CloudTrail es keine Datenereignisse, aber Sie können Trails konfigurieren, um Datenereignisse für S3-Buckets zu protokollieren. Wenn Sie die Protokollierung auf Objektebene für Lesedatenereignisse aktivieren, können Sie jeden einzelnen Objekt- (Datei-) Zugriff innerhalb eines S3-Buckets protokollieren. Durch die Aktivierung der Protokollierung auf Objektebene können Sie mithilfe von Amazon Events Datenkonformitätsanforderungen erfüllen, umfassende Sicherheitsanalysen durchführen AWS-Konto, bestimmte Muster des Benutzerverhaltens in Ihrem System überwachen und Maßnahmen gegen API-Aktivitäten auf Objektebene innerhalb Ihrer S3-Buckets ergreifen. CloudWatch Diese Steuerung führt PASSED zu einem Ergebnis, wenn Sie einen Trail mit mehreren Regionen konfigurieren, der schreibgeschützte oder alle Arten von Datenereignissen für alle S3-Buckets protokolliert.

Abhilfe

Informationen zum Aktivieren der Protokollierung auf Objektebene für S3-Buckets finden Sie unter [Aktivieren der CloudTrail Ereignisprotokollierung für S3-Buckets und Objekte](#) im Amazon Simple Storage Service-Benutzerhandbuch.

[S3.24] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein

Verwandte Anforderungen: PCI DSS v4.0.1/1.4.4

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Hoch

Art der Ressource: `AWS::S3::MultiRegionAccessPoint`

AWS Config Regel: `s3-mrap-public-access-blocked` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für einen Amazon S3 Multiregion Access Point die Einstellungen für den öffentlichen Zugriff blockiert aktiviert sind. Die Kontrolle schlägt fehl, wenn für den Multi-Region Access Point die Einstellungen zum Sperren des öffentlichen Zugriffs nicht aktiviert sind.

Öffentlich zugängliche Ressourcen können zu unberechtigtem Zugriff, Datenschutzverletzungen oder der Ausnutzung von Sicherheitslücken führen. Die Einschränkung des Zugriffs durch Authentifizierungs- und Autorisierungsmaßnahmen trägt zum Schutz vertraulicher Informationen und zur Wahrung der Integrität Ihrer Ressourcen bei.

Abhilfe

Standardmäßig sind alle Einstellungen für den Block Public Access für einen S3-Access Point mit mehreren Regionen aktiviert. Weitere Informationen finden Sie unter [Blockieren des öffentlichen Zugriffs mit Amazon S3 Multi-Region Access Points](#) im Amazon Simple Storage Service-Benutzerhandbuch. Nach dem Erstellen eines Multi-Region Access Point können Sie die Block-Public-Access-Einstellungen für den Access Point nicht mehr ändern.

[S3.25] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben

Kategorie: Schützen > Datenschutz

Schweregrad: Niedrig

Art der Ressource: AWS::S3Express::DirectoryBucket

AWS Config -Regel: [s3express-dir-bucket-lifecycle-rules-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
targetExpirationDays	Die Anzahl der Tage nach der Objekterstellung, an denen Objekte ablaufen sollten.	Ganzzahl	1 auf 2147483647	Kein Standardwert

Dieses Steuerelement prüft, ob Lebenszyklusregeln für einen S3-Verzeichnis-Bucket konfiguriert sind. Die Steuerung schlägt fehl, wenn keine Lebenszyklusregeln für den Directory-Bucket

konfiguriert sind oder eine Lebenszyklusregel für den Bucket Ablaufeinstellungen festlegt, die nicht mit dem Parameterwert übereinstimmen, den Sie optional angeben.

In Amazon S3 besteht eine Lebenszykluskonfiguration aus einer Reihe von Regeln, die Aktionen definieren, die Amazon S3 auf eine Gruppe von Objekten in einem Bucket anwenden soll. Für einen S3-Verzeichnis-Bucket können Sie eine Lebenszyklusregel erstellen, die je nach Alter (in Tagen) festlegt, wann Objekte ablaufen. Sie können auch eine Lebenszyklusregel erstellen, die unvollständige mehrteilige Uploads löscht. Im Gegensatz zu anderen Arten von S3-Buckets, wie z. B. Allzweck-Buckets, unterstützen Directory-Buckets keine anderen Arten von Aktionen für Lebenszyklusregeln, wie z. B. den Übergang von Objekten zwischen Speicherklassen.

Abhilfe

Um eine Lebenszykluskonfiguration für einen S3-Verzeichnis-Bucket zu definieren, erstellen Sie eine Lebenszyklusregel für den Bucket. Weitere Informationen finden Sie unter [Erstellen und Verwalten einer Lebenszykluskonfiguration für Ihren Directory-Bucket](#) im Amazon Simple Storage Service-Benutzerhandbuch.

Security Hub-Steuerungen für SageMaker KI

Diese AWS Security Hub Kontrollen bewerten den Amazon SageMaker AI-Service und die Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben

Verwandte Anforderungen: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.6, PCI DSS v4.0.1/1.4.4

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Hoch

Art der Ressource: AWS::SageMaker::NotebookInstance

AWS Config -Regel: [sagemaker-notebook-no-direct-internet-access](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob der direkte Internetzugang für eine SageMaker KI-Notebook-Instanz deaktiviert ist. Die Steuerung schlägt fehl, wenn das `DirectInternetAccess` Feld für die Notebook-Instanz aktiviert ist.

Wenn Sie Ihre SageMaker AI-Instance ohne VPC konfigurieren, ist der direkte Internetzugang auf Ihrer Instance standardmäßig aktiviert. Sie sollten Ihre Instance mit einer VPC konfigurieren und die Standardeinstellung auf Deaktivieren — Zugriff auf das Internet über eine VPC ändern. Um Modelle von einem Notebook aus zu trainieren oder zu hosten, benötigen Sie Internetzugang. Um den Internetzugang zu aktivieren, muss Ihre VPC entweder über einen Schnittstellenendpunkt (AWS PrivateLink) oder ein NAT-Gateway und eine Sicherheitsgruppe verfügen, die ausgehende Verbindungen zulässt. Weitere Informationen zum Connect einer Notebook-Instance mit Ressourcen in einer VPC finden Sie unter [Verbinden einer Notebook-Instance mit Ressourcen in einer VPC](#) im Amazon SageMaker AI Developer Guide. Sie sollten auch sicherstellen, dass der Zugriff auf Ihre SageMaker KI-Konfiguration nur auf autorisierte Benutzer beschränkt ist. Schränken Sie IAM-Berechtigungen ein, die es Benutzern ermöglichen, SageMaker KI-Einstellungen und -Ressourcen zu ändern.

Abhilfe

Sie können die Internetzugriffseinstellungen nicht ändern, nachdem Sie eine Notebook-Instanz erstellt haben. Stattdessen können Sie die Instanz mit blockiertem Internetzugang beenden, löschen und neu erstellen. Informationen zum Löschen einer Notebook-Instance, die direkten Internetzugang ermöglicht, finden Sie unter [Verwenden von Notebook-Instances zum Erstellen von Modellen: Aufräumen](#) im Amazon SageMaker AI Developer Guide. Informationen zum Neuerstellen einer Notebook-Instance, die den Internetzugang verweigert, finden Sie unter [Notebook-Instance erstellen](#). Wählen Sie für Netzwerk, Direkter Internetzugang die Option Deaktivieren — Zugriff auf das Internet über eine VPC.

[SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden

Verwandte Anforderungen: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen in VPC

Schweregrad: Hoch

Art der Ressource: AWS::SageMaker::NotebookInstance

AWS Config -Regel: [sagemaker-notebook-instance-inside-vpc](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob eine Amazon SageMaker AI-Notebook-Instance in einer benutzerdefinierten Virtual Private Cloud (VPC) gestartet wird. Diese Steuerung schlägt fehl, wenn eine SageMaker KI-Notebook-Instance nicht in einer benutzerdefinierten VPC oder in der SageMaker AI-Service-VPC gestartet wird.

Subnetze sind ein Bereich von IP-Adressen innerhalb einer VPC. Wir empfehlen, Ihre Ressourcen wann immer möglich in einer benutzerdefinierten VPC aufzubewahren, um einen sicheren Netzwerkschutz Ihrer Infrastruktur zu gewährleisten. Eine Amazon VPC ist ein virtuelles Netzwerk, das Ihrem AWS-Konto gewidmet ist. Mit einer Amazon VPC können Sie den Netzwerkzugriff und die Internetverbindung Ihrer SageMaker AI Studio- und Notebook-Instances steuern.

Abhilfe

Sie können die VPC-Einstellung nicht ändern, nachdem Sie eine Notebook-Instanz erstellt haben. Stattdessen können Sie die Instanz beenden, löschen und neu erstellen. Anweisungen finden Sie unter [Verwenden von Notebook-Instances zum Erstellen von Modellen: Aufräumen](#) im Amazon SageMaker AI Developer Guide.

[SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (10), NIST.800-53.r5 AC-6 (2)

Kategorie: Schützen > Sichere Zugriffsverwaltung > Zugriffsbeschränkungen für Root-Benutzer

Schweregrad: Hoch

Art der Ressource: AWS::SageMaker::NotebookInstance

AWS Config -Regel: [sagemaker-notebook-instance-root-access-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der Root-Zugriff für eine Amazon SageMaker AI-Notebook-Instance aktiviert ist. Die Steuerung schlägt fehl, wenn der Root-Zugriff für eine SageMaker AI-Notebook-Instance aktiviert ist.

Unter Einhaltung des Prinzips der geringsten Rechte wird empfohlen, den Root-Zugriff auf Instanzressourcen zu beschränken, um eine unbeabsichtigte Überzuweisung von Zugriffsberechtigungen zu vermeiden.

Abhilfe

Informationen zum Einschränken des Root-Zugriffs auf SageMaker KI-Notebook-Instances finden Sie unter [Steuern des Root-Zugriffs auf eine SageMaker KI-Notebook-Instance](#) im Amazon SageMaker AI Developer Guide.

[SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein

Verwandte Anforderungen: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-5, NIST.800-53.r5 SC-3 6, 3
NIST.800-53.r5 SA-1

Kategorie: Wiederherstellung > Resilienz > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: AWS::SageMaker::EndpointConfig

AWS Config -Regel: [sagemaker-endpoint-config-prod-instance-count](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob Produktionsvarianten eines Amazon SageMaker AI-Endpunkts eine anfängliche Instanzzahl von mehr als 1 aufweisen. Die Kontrolle schlägt fehl, wenn die Produktionsvarianten des Endpunkts nur eine erste Instanz haben.

Produktionsvarianten, die mit einer Instanzzahl von mehr als 1 ausgeführt werden, ermöglichen Multi-AZ-Instance-Redundanz, die von KI verwaltet wird SageMaker . Die Bereitstellung von Ressourcen in mehreren Availability Zones ist eine AWS bewährte Methode, um eine hohe Verfügbarkeit innerhalb Ihrer Architektur zu gewährleisten. Hochverfügbarkeit hilft Ihnen, sich nach Sicherheitsvorfällen zu erholen.

 Note

Diese Steuerung gilt nur für die instanzbasierte Endpunktconfiguration.

Abhilfe

Weitere Informationen zu den Parametern der Endpunktconfiguration finden Sie unter [Erstellen einer Endpunktconfiguration](#) im Amazon SageMaker AI Developer Guide.

[SageMaker.5] SageMaker Modelle sollten eingehenden Datenverkehr blockieren

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Mittel

Art der Ressource: `AWS::SageMaker::Model`

AWS Config -Regel: [sagemaker-model-isolation-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob ein von Amazon SageMaker AI gehostetes Modell eingehenden Netzwerkverkehr blockiert. Die Steuerung schlägt fehl, wenn der `EnableNetworkIsolation` Parameter für das gehostete Modell auf `False` gesetzt ist.

SageMaker KI-Training und bereitgestellte Inferenzcontainer sind standardmäßig internetfähig. Wenn Sie nicht möchten, dass SageMaker KI externen Netzwerkzugriff auf Ihre Trainings- oder Inferenzcontainer gewährt, können Sie die Netzwerkisolierung aktivieren. Wenn Sie die Netzwerkisolierung aktivieren, können die Container keine ausgehenden Netzwerkanrufe tätigen, auch nicht an andere AWS-Services. Darüber hinaus werden der Container-Laufzeitumgebung keine

AWS Anmeldeinformationen zur Verfügung gestellt. Durch die Aktivierung der Netzwerkisolierung wird ein unbeabsichtigter Zugriff auf Ihre SageMaker KI-Ressourcen aus dem Internet verhindert.

Abhilfe

Weitere Informationen zur Netzwerkisolierung für SageMaker KI-Modelle finden Sie unter [Ausführen von Trainings- und Inferenzcontainern im internetfreien Modus](#) im Amazon SageMaker AI Developer Guide. Sie können die Netzwerkisolierung aktivieren, wenn Sie Ihren Trainingsjob oder Ihr Trainingsmodell erstellen, indem Sie den Wert des `EnableNetworkIsolation` Parameters auf `True` setzen.

[SageMaker.6] SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::SageMaker::AppImageConfig`

AWS Config -Regel: [sagemaker-app-image-config-tagged](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Eine Liste der Tag-Schlüssel vom Typ „“, die einer ausgewerteten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon SageMaker AI-App-Image-Konfiguration (AppImageConfig) die durch den `requiredKeyTags` Parameter angegebenen Tag-Schlüssel enthält. Die Steuerung schlägt fehl, wenn die Konfiguration des App-Images keine Tag-Schlüssel oder nicht alle im `requiredKeyTags` Parameter angegebenen Schlüssel enthält. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die App-Image-Konfiguration keine Tag-Schlüssel enthält. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws:` Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im [Tagging AWS Resources and Tag](#) Editor User Guide.

Note

Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Um einer Amazon SageMaker AI-App-Image-Konfiguration (AppImageConfig) Tags hinzuzufügen, können Sie den [AddTags](#) Betrieb der SageMaker KI-API verwenden oder, falls Sie die verwenden AWS CLI, den Befehl [add-tags](#) ausführen.

[SageMaker.7] SageMaker Bilder sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::SageMaker::Image

AWS Config -Regel: [sagemaker-image-tagged](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Eine Liste der Tag-Schlüssel vom Typ „“, die einer ausgewerteten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon SageMaker AI-Bild die durch den `requiredKeyTags` Parameter angegebenen Tag-Schlüssel hat. Die Steuerung schlägt fehl, wenn das Bild keine Tag-Schlüssel oder nicht alle im `requiredKeyTags` Parameter angegebenen Schlüssel hat. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Bild keine Tagschlüssel hat. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws:` Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im [Tagging AWS Resources and Tag](#) Editor User Guide.

 Note

Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Um einem Amazon SageMaker AI-Image Tags hinzuzufügen, können Sie den [AddTags](#) Betrieb der SageMaker KI-API verwenden oder, falls Sie die verwenden AWS CLI, den Befehl [add-tags](#) ausführen.

[SageMaker.8] SageMaker Notebook-Instances sollten auf unterstützten Plattformen laufen

Kategorie: Erkennen > Schwachstellen-, Patch- und Versionsverwaltung

Schweregrad: Mittel

Art der Ressource: AWS::SageMaker::NotebookInstance

AWS Config -Regel: [sagemaker-notebook-instance-platform-version](#)

Art des Zeitplans: Periodisch

Parameter:

- supportedPlatformIdentifizierVersions: notebook-a12-v3 (nicht anpassbar)

Dieses Steuerelement prüft anhand der für die Notebook-Instance angegebenen Plattform-ID, ob eine Amazon SageMaker AI-Notebook-Instance für die Ausführung auf einer unterstützten Plattform konfiguriert ist. Die Steuerung schlägt fehl, wenn die Notebook-Instance für die Ausführung auf einer Plattform konfiguriert ist, die nicht mehr unterstützt wird.

Wenn die Plattform für eine Amazon SageMaker AI-Notebook-Instance nicht mehr unterstützt wird, erhält sie möglicherweise keine Sicherheitspatches, Bugfixes oder andere Arten von Updates. Notebook-Instances funktionieren möglicherweise weiterhin, erhalten jedoch keine SageMaker KI-Sicherheitsupdates oder kritische Bugfixes. Sie übernehmen die Risiken, die mit der Verwendung

einer nicht unterstützten Plattform verbunden sind. Weitere Informationen finden Sie unter [JupyterLabVersionierung](#) im Amazon SageMaker AI Developer Guide.

Abhilfe

Informationen zu den Plattformen, die Amazon SageMaker AI derzeit unterstützt, und zur Migration zu diesen Plattformen finden Sie unter [Amazon Linux 2-Notebook-Instances](#) im Amazon SageMaker AI Developer Guide.

Security Hub-Steuerelemente für Secrets Manager

Diese AWS Security Hub Kontrollen bewerten den AWS Secrets Manager Service und die Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[SecretsManager.1] Bei Secrets Manager Manager-Geheimnissen sollte die automatische Rotation aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), PCI DSS v4.0.1/8.6.3, PCI DSS v4.0.1/8.3.9

Kategorie: Schutz > Sichere Entwicklung

Schweregrad: Mittel

Art der Ressource: AWS::SecretsManager::Secret

AWS Config -Regel: [secretsmanager-rotation-enabled-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
maximumAllowedRotationFrequency	Maximale Anzahl von Tagen, die für die geheime Rotationsfrequenz zulässig sind	Ganzzahl	1 auf 365	Kein Standardwert

Dieses Steuerelement prüft, ob ein in gespeichertes Geheimnis mit automatischer Rotation konfiguriert AWS Secrets Manager ist. Die Steuerung schlägt fehl, wenn das Geheimnis nicht mit automatischer Rotation konfiguriert ist. Wenn Sie einen benutzerdefinierten Wert für den `maximumAllowedRotationFrequency` Parameter angeben, ist die Kontrolle nur erfolgreich, wenn das Geheimnis innerhalb des angegebenen Zeitfensters automatisch rotiert wird.

Secrets Manager hilft Ihnen, die Sicherheitslage Ihres Unternehmens zu verbessern. Zu den Geheimnissen gehören Datenbankanmeldedaten, Passwörter und API-Schlüssel von Drittanbietern. Sie können Secrets Manager verwenden, um Secrets zentral zu speichern, Secrets automatisch zu verschlüsseln, den Zugriff auf Secrets zu kontrollieren und Secrets sicher und automatisch zu rotieren.

Secrets Manager kann Secrets rotieren. Sie können die Rotation verwenden, um langfristige Geheimnisse durch kurzfristige zu ersetzen. Durch die Rotation Ihrer Geheimnisse wird begrenzt, wie lange ein nicht autorisierter Benutzer ein kompromittiertes Geheimnis verwenden kann. Aus diesem Grund sollten Sie Ihre Geheimnisse häufig wechseln. Weitere Informationen zur Rotation findest du unter [Rotation deiner AWS Secrets Manager Geheimnisse](#) im AWS Secrets Manager Benutzerhandbuch.

Abhilfe

Informationen zum Aktivieren der automatischen Rotation für Secrets Manager-Secrets finden Sie unter [Automatische Rotation für AWS Secrets Manager Secrets mithilfe der Konsole einrichten](#) im AWS Secrets Manager Benutzerhandbuch. Sie müssen eine AWS Lambda Funktion für die Rotation auswählen und konfigurieren.

[SecretsManager.2] Secrets Manager Manager-Geheimnisse, die mit automatischer Rotation konfiguriert sind, sollten erfolgreich rotieren

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), PCI DSS v4.0.1/8.6.3, PCI DSS v4.0.1/8.3.9

Kategorie: Schutz > Sichere Entwicklung

Schweregrad: Mittel

Art der Ressource: AWS::SecretsManager::Secret

AWS Config -Regel: [secretsmanager-scheduled-rotation-success-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft anhand des Rotationsplans, ob ein AWS Secrets Manager Secret erfolgreich rotiert wurde. Wenn `RotationOccurringAsScheduled` ja, schlägt die Steuerung fehlfalse. Das Steuerelement wertet nur Geheimnisse aus, für die die Rotation aktiviert ist.

Secrets Manager hilft Ihnen, die Sicherheitslage Ihres Unternehmens zu verbessern. Zu den Geheimnissen gehören Datenbankanmeldedaten, Passwörter und API-Schlüssel von Drittanbietern. Sie können Secrets Manager verwenden, um Secrets zentral zu speichern, Secrets automatisch zu verschlüsseln, den Zugriff auf Secrets zu kontrollieren und Secrets sicher und automatisch zu rotieren.

Secrets Manager kann Secrets rotieren. Sie können die Rotation verwenden, um langfristige Geheimnisse durch kurzfristige zu ersetzen. Durch die Rotation Ihrer Geheimnisse wird begrenzt, wie lange ein nicht autorisierter Benutzer ein kompromittiertes Geheimnis verwenden kann. Aus diesem Grund sollten Sie Ihre Geheimnisse häufig wechseln.

Zusätzlich zur Konfiguration der automatischen Rotation sollten Sie sicherstellen, dass diese Secrets gemäß dem Rotationsplan erfolgreich rotiert werden.

Weitere Informationen zur Rotation finden Sie unter [Rotation Ihrer AWS Secrets Manager Geheimnisse](#) im AWS Secrets Manager Benutzerhandbuch.

Abhilfe

Wenn die automatische Rotation fehlschlägt, sind bei Secrets Manager möglicherweise Fehler bei der Konfiguration aufgetreten. Um Secrets in Secrets Manager zu rotieren, verwenden Sie eine

Lambda-Funktion, die definiert, wie mit der Datenbank oder dem Dienst, dem das Geheimnis gehört, interagiert werden soll.

Hilfe zur Diagnose und Behebung häufiger Fehler im Zusammenhang mit der Rotation von Geheimnissen finden Sie unter [Fehlerbehebung bei der AWS Secrets Manager Rotation von Geheimnissen](#) im AWS Secrets Manager Benutzerhandbuch.

[SecretsManager.3] Unbenutzte Secrets Manager Manager-Geheimnisse entfernen

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15)

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: AWS::SecretsManager::Secret

AWS Config -Regel: [secretsmanager-secret-unused](#)

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
unusedForDays	Maximale Anzahl von Tagen, an denen ein Geheimnis ungenutzt bleiben kann	Ganzzahl	1 auf 365	90

Dieses Steuerelement prüft, ob innerhalb des angegebenen Zeitraums auf ein AWS Secrets Manager Geheimnis zugegriffen wurde. Die Kontrolle schlägt fehl, wenn ein Geheimnis über den angegebenen Zeitraum hinaus nicht verwendet wird. Sofern Sie keinen benutzerdefinierten Parameterwert für den Zugriffszeitraum angeben, verwendet Security Hub einen Standardwert von 90 Tagen.

Das Löschen ungenutzter Geheimnisse ist genauso wichtig wie das Rotieren von Geheimnissen. Ungenutzte Geheimnisse können von ihren früheren Benutzern missbraucht werden, die keinen Zugriff mehr auf diese Geheimnisse benötigen. Da immer mehr Benutzer Zugriff auf ein Geheimnis

erhalten, könnte es außerdem sein, dass jemand es falsch behandelt und an eine nicht autorisierte Stelle weitergegeben hat, was das Missbrauchsrisiko erhöht. Das Löschen ungenutzter Geheimnisse hilft dabei, Benutzern, die ihn nicht mehr benötigen, den geheimen Zugriff zu entziehen. Es hilft auch, die Kosten für die Verwendung von Secrets Manager zu senken. Daher ist es wichtig, ungenutzte Geheimnisse routinemäßig zu löschen.

Abhilfe

Informationen zum Löschen inaktiver Secrets Manager-Geheimnisse finden [Sie unter Löschen eines AWS Secrets Manager Geheimnisses](#) im AWS Secrets Manager Benutzerhandbuch.

[SecretsManager.4] Secrets Manager Manager-Geheimnisse sollten innerhalb einer bestimmten Anzahl von Tagen rotiert werden

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), PCI DSS v4.0.1/8.6.3, PCI DSS v4.0.1/8.3.9

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: AWS::SecretsManager::Secret

AWS Config -Regel: [secretsmanager-secret-periodic-rotation](#)

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
maxDaysSinceRotation	Maximale Anzahl von Tagen, an denen ein Geheimnis unverändert bleiben kann	Ganzzahl	1 auf 180	90

Dieses Steuerelement prüft, ob ein AWS Secrets Manager Geheimnis innerhalb des angegebenen Zeitrahmens mindestens einmal rotiert wurde. Die Kontrolle schlägt fehl, wenn ein Geheimnis nicht

mindestens so häufig gewechselt wird. Sofern Sie keinen benutzerdefinierten Parameterwert für den Rotationszeitraum angeben, verwendet Security Hub einen Standardwert von 90 Tagen.

Rotierende Geheimnisse können Ihnen helfen, das Risiko einer unbefugten Verwendung Ihrer Geheimnisse in Ihrem zu verringern AWS-Konto. Beispiele hierfür sind Datenbankanmeldedaten, Passwörter, API-Schlüssel von Drittanbietern und sogar beliebiger Text. Wenn Sie Ihre Geheimnisse über einen längeren Zeitraum nicht ändern, ist es wahrscheinlicher, dass die Geheimnisse kompromittiert werden.

Je mehr Benutzer Zugriff auf ein Geheimnis erhalten, desto wahrscheinlicher kann es sein, dass jemand falsch damit umgegangen ist und es an eine nicht autorisierte Person weitergegeben hat. Secrets können über Protokolle und Cache-Daten durchsickern. Sie werden ggf. für Debug-Zwecke freigegeben und nicht geändert oder widerrufen, wenn das Debugging abgeschlossen ist. Aus all diesen Gründen sollten Secrets regelmäßig rotiert werden.

Sie können die automatische Rotation von Geheimnissen konfigurieren. AWS Secrets Manager Mit der automatischen Rotation können Sie langfristige Geheimnisse durch kurzfristige ersetzen, wodurch das Risiko von Kompromissen erheblich reduziert wird. Wir empfehlen Ihnen, die automatische Rotation für Ihre Secrets Manager zu konfigurieren. Weitere Informationen finden Sie unter [Rotieren von AWS Secrets Manager -Secrets](#) im AWS Secrets Manager -Benutzerhandbuch.

Abhilfe

Informationen zum Aktivieren der automatischen Rotation für Secrets Manager-Secrets finden Sie unter [Automatische Rotation für AWS Secrets Manager Secrets mithilfe der Konsole einrichten](#) im AWS Secrets Manager Benutzerhandbuch. Sie müssen eine AWS Lambda Funktion für die Rotation auswählen und konfigurieren.

[SecretsManager.5] Secrets Manager Manager-Geheimnisse sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::SecretsManager::Secret

AWS Config Regel: tagged-secretsmanager-secret (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob ein AWS Secrets Manager Secret Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn das Geheimnis keine Tagschlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel enthält `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Geheimnis mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` beginnen, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Secrets Manager Manager-Geheimnis finden Sie unter [AWS Secrets Manager Taggeheimnisse](#) im AWS Secrets Manager Benutzerhandbuch.

Security Hub-Steuerungen für AWS Service Catalog

Dieses AWS Security Hub Steuerelement bewertet den AWS Service Catalog Dienst und die Ressourcen. Das Steuerelement ist möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden

Verwandte Anforderungen: NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-6, NIST.800-53.r5 CM-8, NIST.800-53.r5 SC-7

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Hoch

Art der Ressource: AWS::ServiceCatalog::Portfolio

AWS Config -Regel: [service-catalog-shared-within-organization](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob AWS Service Catalog Portfolios innerhalb einer Organisation gemeinsam genutzt werden, wenn die Integration mit aktiviert AWS Organizations ist. Die Kontrolle schlägt fehl, wenn Portfolios nicht innerhalb einer Organisation gemeinsam genutzt werden.

Die Portfoliofreigabe nur innerhalb von Organizations trägt dazu bei, dass ein Portfolio nicht mit falschen Personen geteilt wird AWS-Konten. Um ein Servicekatalog-Portfolio mit einem Konto in einer Organisation zu teilen, empfiehlt Security Hub die Verwendung von `ORGANIZATION_MEMBER_ACCOUNT` anstelle von `ACCOUNT`. Dies vereinfacht die Verwaltung, da der Zugriff, der dem Konto gewährt wird, unternehmensweit geregelt wird. Wenn Sie aus geschäftlichen Gründen Service Catalog-Portfolios mit einem externen Konto teilen müssen, können Sie [die Ergebnisse dieser Steuerung automatisch unterdrücken](#) oder [deaktivieren](#).

Abhilfe

Informationen zum Aktivieren der Portfolio-Sharing mit AWS Organizations finden Sie unter [Teilen mit AWS Organizations](#) im AWS Service Catalog Administratorhandbuch.

Security Hub-Steuerelemente für Amazon SES

Diese AWS Security Hub Kontrollen bewerten den Service und die Ressourcen von Amazon Simple Email Service (Amazon SES).

Diese Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[SES.1] SES-Kontaktlisten sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::SES::ContactList`

AWS Config Regel: `tagged-ses-contactlist` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon SES SES-Kontaktliste Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind `requiredTagKeys`. Die Kontrolle schlägt fehl, wenn die Kontaktliste keine Tag-Schlüssel enthält oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Kontaktliste mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Amazon SES-Kontaktliste finden Sie [TagResource](#) in der Amazon SES API v2-Referenz.

[SES.2] SES-Konfigurationssätze sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Kennzeichnung

Schweregrad: Niedrig

Art der Ressource: `AWS::SES::ConfigurationSet`

AWS Config Regel: `tagged-ses-configurationset` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon SES SES-Konfigurationssatz Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind `requiredTagKeys`. Die Steuerung schlägt fehl, wenn der Konfigurationssatz keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Konfigurationssatz mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :` , werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Amazon SES-Konfigurationssatz finden Sie [TagResource](#) in der Amazon SES API v2-Referenz.

Security Hub-Steuerelemente für Amazon SNS

Diese AWS Security Hub Kontrollen bewerten den Service und die Ressourcen des Amazon Simple Notification Service (Amazon SNS). Die Kontrollen sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[SNS.1] SNS-Themen sollten im Ruhezustand wie folgt verschlüsselt werden AWS KMS

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8 (1), (10), NIST.800-53.R5 NIST.800-53.r5 SC-2 SI-7 (6), NIST.800-53.r5 SC-7 NIST.800-171.r2 3.13.11, NIST.800-171.R2 3.13.16

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: AWS::SNS::Topic

AWS Config -Regel: [sns-encrypted-kms](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon SNS SNS-Thema im Ruhezustand mithilfe von Schlüsseln verschlüsselt ist, die in AWS Key Management Service (AWS KMS) verwaltet werden. Die Steuerung schlägt fehl, wenn das SNS-Thema keinen KMS-Schlüssel für die serverseitige Verschlüsselung (SSE) verwendet. Standardmäßig speichert SNS Nachrichten und Dateien mithilfe der Festplattenverschlüsselung. Um diese Kontrolle zu bestehen, müssen Sie stattdessen einen KMS-Schlüssel für die Verschlüsselung verwenden. Dies fügt eine zusätzliche Sicherheitsebene hinzu und bietet mehr Flexibilität bei der Zugriffskontrolle.

Durch die Verschlüsselung von Daten im Ruhezustand wird das Risiko verringert, dass auf Daten, die auf der Festplatte gespeichert sind, von einem Benutzer zugegriffen wird, für den kein Benutzer authentifiziert ist. AWS API-Berechtigungen sind erforderlich, um die Daten zu entschlüsseln, bevor sie gelesen werden können. Wir empfehlen, SNS-Themen mit KMS-Schlüsseln zu verschlüsseln, um eine zusätzliche Sicherheitsebene zu gewährleisten.

Abhilfe

Informationen zur Aktivierung von SSE für ein SNS-Thema finden Sie unter [Aktivieren der serverseitigen Verschlüsselung \(SSE\) für ein Amazon SNS SNS-Thema](#) im Amazon Simple Notification Service Developer Guide. Bevor Sie SSE verwenden können, müssen Sie außerdem AWS KMS key Richtlinien konfigurieren, die die Verschlüsselung von Themen sowie die Verschlüsselung und Entschlüsselung von Nachrichten ermöglichen. Weitere Informationen finden

Sie unter [Konfiguration von AWS KMS Berechtigungen](#) im Amazon Simple Notification Service Developer Guide.

[SNS.2] Die Protokollierung des Lieferstatus sollte für Benachrichtigungen aktiviert werden, die an ein Thema gesendet werden

 Important

Security Hub hat diese Kontrolle im April 2024 eingestellt. Weitere Informationen finden Sie unter [Änderungsprotokoll für Security Hub CSPM-Steuerelemente](#).

Verwandte Anforderungen: NIST.800-53.R5 AU-12, NIST.800-53.R5 AU-2

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS::SNS::Topic

AWS Config -Regel: [sns-topic-message-delivery-notification-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Protokollierung für den Lieferstatus von Benachrichtigungen aktiviert ist, die an ein Amazon SNS SNS-Thema für die Endgeräte gesendet werden. Diese Kontrolle schlägt fehl, wenn die Benachrichtigung über den Lieferstatus von Nachrichten nicht aktiviert ist.

Die Protokollierung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von Diensten. Die Protokollierung des Nachrichtenzustellungsstatus hilft dabei, betriebliche Erkenntnisse wie die folgenden zu gewinnen:

- Kenntnis, ob eine Mitteilung an den Amazon SNS-Endpunkt gesendet wurde.
- Ermittlung der Antwort, die vom Amazon SNS-Endpunkt an Amazon SNS gesendet wurde.
- Bestimmung der Verweildauer der Nachricht (die Zeit zwischen dem Veröffentlichungszeitstempel und der Übergabe an einen Amazon SNS SNS-Endpunkt).

Abhilfe

Informationen zur Konfiguration der Versandstatusprotokollierung für ein Thema finden Sie unter [Amazon SNS SNS-Nachrichtenzustellungsstatus](#) im Amazon Simple Notification Service Developer Guide.

[SNS.3] SNS-Themen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::SNS::Topic`

AWS Config Regel: `tagged-sns-topic` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob ein Amazon SNS SNS-Thema Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn das Thema keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Thema mit keinem Schlüssel markiert ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem SNS-Thema finden Sie unter [Konfiguration von Amazon SNS SNS-Themen-Tags](#) im Amazon Simple Notification Service Developer Guide.

[SNS.4] Zugriffsrichtlinien für SNS-Themen sollten keinen öffentlichen Zugriff zulassen

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Hoch

Art der Ressource: `AWS::SNS::Topic`

AWS Config -Regel: [sns-topic-no-public-access](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob die Amazon SNS SNS-Themenzugriffsrichtlinie öffentlichen Zugriff zulässt. Diese Kontrolle schlägt fehl, wenn die SNS-Themenzugriffsrichtlinie den öffentlichen Zugriff zulässt.

Sie verwenden eine Amazon SNS SNS-Zugriffsrichtlinie mit einem bestimmten Thema, um einzuschränken, wer mit diesem Thema arbeiten kann (z. B. wer Nachrichten zu diesem Thema veröffentlichen oder wer es abonnieren kann). SNS-Richtlinien können anderen AWS-Konten oder Benutzern innerhalb Ihres eigenen Bereichs Zugriff gewähren. AWS-Konto Die Angabe eines Platzhalters (*) im `Principal` Feld der Themenrichtlinie und das Fehlen von Bedingungen zur Einschränkung der Themenrichtlinie können zu Datenexfiltration, Denial-of-Service oder unerwünschter Einschleusung von Nachrichten in Ihren Dienst durch einen Angreifer führen.

Note

Dieses Steuerelement bewertet keine Richtlinienbedingungen, die Platzhalterzeichen oder Variablen verwenden. Um ein PASSED Ergebnis zu erzielen, dürfen Bedingungen in der Amazon SNS SNS-Zugriffsrichtlinie für ein Thema nur feste Werte verwenden, d. h. Werte, die keine Platzhalterzeichen oder Richtlinienvariablen enthalten. Informationen zu Richtlinienvariablen finden Sie unter [Variablen und Tags](#) im AWS Identity and Access Management Benutzerhandbuch.

Abhilfe

Informationen zur Aktualisierung der Zugriffsrichtlinien für ein SNS-Thema finden Sie unter [Überblick über die Zugriffsverwaltung in Amazon SNS](#) im Amazon Simple Notification Service Developer Guide.

Security Hub-Steuerelemente für Amazon SQS

Diese AWS Security Hub Kontrollen bewerten den Service und die Ressourcen des Amazon Simple Queue Service (Amazon SQS). Die Kontrollen sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 (1), (10), NIST.800-53.R5 NIST.800-53.r5 SC-2 SI-7 NIST.800-53.r5 SC-7 (6)

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: AWS::SQS::Queue

AWS Config Regel: sqs-queue-encrypted (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Amazon SQS SQS-Warteschlange im Ruhezustand verschlüsselt ist. Die Steuerung schlägt fehl, wenn die Warteschlange nicht mit einem von SQL verwalteten Schlüssel (SSE-SQS) oder einem AWS Key Management Service () Schlüssel (SSE-KMS) verschlüsselt ist. AWS KMS

Durch die Verschlüsselung von Daten im Ruhezustand wird das Risiko verringert, dass ein nicht autorisierter Benutzer auf Daten zugreift, die auf der Festplatte gespeichert sind. Die serverseitige Verschlüsselung (SSE) schützt den Inhalt von Nachrichten in SQS-Warteschlangen mithilfe von SQS-verwalteten Verschlüsselungsschlüsseln (SSE-SQS) oder Schlüsseln (SSE-KMS). AWS KMS

Abhilfe

Informationen zur Konfiguration von SSE für eine SQS-Warteschlange finden Sie unter [Konfiguration der serverseitigen Verschlüsselung \(SSE\) für eine Warteschlange \(Konsole\)](#) im Amazon Simple Queue Service Developer Guide.

[SQS.2] SQS-Warteschlangen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::SQS::Queue

AWS Config Regel: tagged-sqs-queue (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob eine Amazon SQS SQS-Warteschlange Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn die Warteschlange keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Warteschlange mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer vorhandenen Warteschlange mithilfe der Amazon SQS SQS-Konsole finden Sie unter [Konfiguration von Kostenzuweisungs-Tags für eine Amazon SQS SQS-Warteschlange \(Konsole\)](#) im Amazon Simple Queue Service Developer Guide.

[SQS.3] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen

Kategorie: Schützen > Sichere Zugriffsverwaltung > Ressource nicht öffentlich zugänglich

Schweregrad: Hoch

Art der Ressource: AWS::SQS::Queue

AWS Config -Regel: [sqs-queue-no-public-access](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob eine Amazon SQS SQS-Zugriffsrichtlinie öffentlichen Zugriff auf eine SQS-Warteschlange ermöglicht. Die Kontrolle schlägt fehl, wenn eine SQS-Zugriffsrichtlinie öffentlichen Zugriff auf die Warteschlange ermöglicht.

Eine Amazon SQS SQS-Zugriffsrichtlinie kann den öffentlichen Zugriff auf eine SQS-Warteschlange ermöglichen, was einem anonymen Benutzer oder einer authentifizierten AWS IAM-Identität den Zugriff auf die Warteschlange ermöglichen kann. SQS-Zugriffsrichtlinien ermöglichen diesen Zugriff in der Regel durch Angabe des Platzhalterzeichens (*) im Principal Element der Richtlinie, ohne dass die richtigen Bedingungen verwendet werden, um den Zugriff auf die Warteschlange einzuschränken, oder beides. Wenn eine SQS-Zugriffsrichtlinie öffentlichen Zugriff zulässt, können Dritte möglicherweise Aufgaben wie das Empfangen von Nachrichten aus der Warteschlange,

das Senden von Nachrichten an die Warteschlange oder das Ändern der Zugriffsrichtlinie für die Warteschlange ausführen. Dies kann zu Ereignissen wie Datenexfiltration, einem Denial-of-Service oder der Einschleusung von Nachrichten in die Warteschlange durch einen Bedrohungsakteur führen.

Note

Dieses Steuerelement bewertet keine Richtlinienbedingungen, die Platzhalterzeichen oder Variablen verwenden. Um ein PASSED Ergebnis zu erzielen, dürfen Bedingungen in der Amazon SQS SQS-Zugriffsrichtlinie für eine Warteschlange nur feste Werte verwenden, d. h. Werte, die keine Platzhalterzeichen oder Richtlinienvariablen enthalten. Informationen zu Richtlinienvariablen finden Sie unter [Variablen und Tags](#) im AWS Identity and Access Management Benutzerhandbuch.

Abhilfe

Informationen zur Konfiguration der SQS-Zugriffsrichtlinie für eine SQS-Warteschlange finden Sie unter [Using custom policies with the Amazon SQS Access Policy Language](#) im Amazon Simple Queue Service Developer Guide.

Security Hub-Steuerelemente für Step Functions

Diese AWS Security Hub Kontrollen bewerten den AWS Step Functions Service und die Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[StepFunctions.1] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben

Verwandte Anforderungen: PCI DSS v4.0.1/10.4.2

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS::StepFunctions::StateMachine

AWS Config -Regel: [step-functions-state-machine-logging-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
logLevel	Minimale Protokollierungsebene	Enum	ALL, ERROR, FATAL	Kein Standardwert

Mit dieser Steuerung wird geprüft, ob bei einer AWS Step Functions Zustandsmaschine die Protokollierung aktiviert ist. Die Steuerung schlägt fehl, wenn für eine Zustandsmaschine die Protokollierung nicht aktiviert ist. Wenn Sie einen benutzerdefinierten Wert für den `logLevel` Parameter angeben, wird die Steuerung nur erfolgreich ausgeführt, wenn für die Zustandsmaschine die angegebene Protokollierungsebene aktiviert ist.

Die Überwachung hilft Ihnen dabei, die Zuverlässigkeit, Verfügbarkeit und Leistung von Step Functions aufrechtzuerhalten. Sie sollten so viele Überwachungsdaten sammeln AWS-Services, wie Sie verwenden, damit Sie Fehler an mehreren Punkten leichter debuggen können. Wenn Sie eine Protokollierungskonfiguration für Ihre Step Functions Functions-Zustandsmaschinen definiert haben, können Sie den Ausführungsverlauf und die Ergebnisse in Amazon CloudWatch Logs verfolgen. Optional können Sie nur Fehler oder schwerwiegende Ereignisse verfolgen.

Abhilfe

Informationen zum Aktivieren der Protokollierung für eine Step Functions Functions-Zustandsmaschine finden [Sie unter Protokollierung konfigurieren](#) im AWS Step Functions Entwicklerhandbuch.

[StepFunctions.2] Die Aktivitäten von Step Functions sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::StepFunctions::Activity`

AWS Config Regel: tagged-stepfunctions-activity (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS Step Functions Aktivität Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn die Aktivität keine Tag-Schlüssel hat oder wenn nicht alle im Parameter angegebenen Schlüssel vorhanden sind `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Aktivität mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginaws :`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen

möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

Note

Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Step Functions-Aktivität finden Sie unter [Tagging in Step Functions](#) im AWS Step Functions Entwicklerhandbuch.

Security Hub-Steuerelemente für Systems Manager

Diese AWS Security Hub Kontrollen bewerten den AWS Systems Manager (SSM) -Service und die Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[SSM.1] EC2 Amazon-Instances sollten verwaltet werden von AWS Systems Manager

Verwandte Anforderungen: PCI DSS v3.2.1/2.4, NIST.800-53.r5 CA-9 (1), 5 (2), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-8, NIST.800-53.r5 CM-8(1), NIST.800-53.r5 CM-8(2), NIST.800-53.r5 CM-8(3), NIST.800-53.r5 SA-1 5 (8), NIST.800-53.r5 SA-1 NIST.800-53.R5 SI-2 (3) NIST.800-53.r5 SA-3

Kategorie: Identifizieren > Bestand

Schweregrad: Mittel

Evaluierte Ressource: AWS::EC2::Instance

Erforderliche AWS Config Aufzeichnungsressourcen: AWS::EC2::Instance,
AWS::SSM::ManagedInstanceInventory

AWS Config -Regel: [ec2-instance-managed-by-systems-manager](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die gestoppten und laufenden EC2 Instances in Ihrem Konto von verwaltet werden AWS Systems Manager. Systems Manager ist ein AWS-Service Programm, mit dem Sie Ihre AWS Infrastruktur anzeigen und steuern können.

Um Sie bei der Aufrechterhaltung von Sicherheit und Compliance zu unterstützen, scannt Systems Manager Ihre gestoppten und laufenden verwalteten Instances. Eine verwaltete Instanz ist eine Maschine, die für die Verwendung mit Systems Manager konfiguriert ist. Systems Manager meldet dann alle festgestellten Richtlinienverstöße oder ergreift Korrekturmaßnahmen. Systems Manager hilft Ihnen auch bei der Konfiguration und Wartung Ihrer verwalteten Instanzen.

Weitere Informationen finden Sie im [AWS Systems Manager Benutzerhandbuch](#).

Abhilfe

Informationen zur Verwaltung von EC2 Instances mit Systems Manager finden Sie unter [Amazon EC2 Host Management](#) im AWS Systems Manager Benutzerhandbuch. Im Abschnitt Konfigurationsoptionen können Sie die Standardoptionen beibehalten oder sie nach Bedarf für Ihre bevorzugte Konfiguration ändern.

[SSM.2] Von Systems Manager verwaltete EC2 Amazon-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben

Verwandte Anforderungen: NIST.800-53.R5 CM-8 (3), NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (3), NIST.800-53.R5 SI-2 (4), NIST.800-53.R5 SI-2 (5), NIST.800-171.r2 3.7.1, PCI DSS v3.2.1/6.2, PCI DSS v4.0.1/2.2.1, PCI DSS v4.0.1/6.3.3

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Hoch

Art der Ressource: AWS::SSM::PatchCompliance

AWS Config -Regel: [ec2-managedinstance-patch-compliance-status-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement überprüft, ob der Konformitätsstatus von Systems Manager Patch Compliance COMPLIANT oder NON_COMPLIANT nach der Patch-Installation auf der Instanz ist. Die Kontrolle

schlägt fehl, wenn der Konformitätsstatus lautet `NON_COMPLIANT`. Das Steuerelement überprüft nur Instanzen, die von Systems Manager Patch Manager verwaltet werden.

Durch das Patchen Ihrer EC2 Instanzen nach den Anforderungen Ihres Unternehmens wird die Angriffsfläche Ihrer AWS-Konten Instanzen reduziert.

Abhilfe

Systems Manager empfiehlt die Verwendung von [Patch-Richtlinien](#), um das Patchen für Ihre verwalteten Instanzen zu konfigurieren. Sie können auch [Systems Manager Manager-Dokumente](#) verwenden, wie im folgenden Verfahren beschrieben, um eine Instanz zu patchen.

So korrigieren Sie nicht konforme Patches

1. Öffnen Sie die AWS Systems Manager Konsole unter <https://console.aws.amazon.com/systems-manager/>.
2. Wählen Sie für Node Management die Option Befehl ausführen und anschließend Befehl ausführen aus.
3. Wählen Sie die Option für AWS- RunPatchBaseline.
4. Ändern Sie die Operation in Install (Installieren).
5. Wählen Sie Instanzen manuell auswählen und wählen Sie dann die nicht konformen Instanzen aus.
6. Wählen Sie Ausführen aus.
7. Wenn der Befehl abgeschlossen ist, wählen Sie im Navigationsbereich Compliance aus, um den neuen Compliance-Status Ihrer gepatchten Instances zu überwachen.

[SSM.3] Von Systems Manager verwaltete EC2 Amazon-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2), NIST.800-53.R5 CM-8, NIST.800-53.R5 CM-8 (1), NIST.800-53.R5 CM-8 (3), NIST.800-53.r5 SI-2 (3), PCI DSS v3.2.1/2.4, PCI DSS v4.0.1/2.2.1, PCI DSS v4.0.1/6.3.3

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Art der Ressource: `AWS::SSM::AssociationCompliance`

AWS Config -Regel: [ec2-managedinstance-association-compliance-status-check](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Mit diesem Steuerelement wird geprüft, ob der Status der AWS Systems Manager Zuordnung auf einer Instanz den Status „Konformität“ hat COMPLIANT oder NON_COMPLIANT nachdem die Zuordnung ausgeführt wurde. Die Kontrolle schlägt fehl, wenn der Konformitätsstatus der Assoziation lautetNON_COMPLIANT.

Eine State Manager-Zuordnung ist eine Konfiguration, die Ihren verwalteten Instances zugewiesen ist. Die Konfiguration definiert den Status, den Sie auf Ihren Instances beibehalten möchten. Eine Zuordnung kann beispielsweise angeben, dass Antivirensoftware auf Ihren Instanzen installiert und ausgeführt werden muss oder dass bestimmte Ports geschlossen sein müssen.

Nachdem Sie eine oder mehrere State Manager-Zuordnungen erstellt haben, stehen Ihnen sofort Informationen zum Compliance-Status zur Verfügung. Sie können den Konformitätsstatus in der Konsole oder als Reaktion auf AWS CLI Befehle oder entsprechende Systems Manager API-Aktionen anzeigen. Bei Zuordnungen zeigt Configuration Compliance den Konformitätsstatus (CompliantoderNon-compliant) an. Außerdem wird der Schweregrad angezeigt, der der Zuordnung zugewiesen wurde, z. B. Critical oderMedium.

Weitere Informationen zur Einhaltung der State Manager-Zuordnungen finden Sie im AWS Systems Manager Benutzerhandbuch unter [Informationen zur Einhaltung von State Manager-Zuordnungen](#).

Abhilfe

Eine fehlgeschlagene Zuordnung kann auf verschiedene Dinge zurückzuführen sein, z. B. auf Ziele und Systems Manager Manager-Dokumentnamen. Um dieses Problem zu beheben, müssen Sie zunächst die Zuordnung identifizieren und untersuchen, indem Sie sich den Zuordnungsverlauf ansehen. Anweisungen zum Anzeigen des Zuordnungsverlaufs finden Sie unter [Zuordnungshistorien](#) anzeigen im AWS Systems Manager Benutzerhandbuch.

Nach der Untersuchung können Sie die Zuordnung bearbeiten, um das festgestellte Problem zu beheben. Sie können eine Zuordnung bearbeiten, um den Namen, den Zeitplan, den Schweregrad oder die Ziele zu ändern. Nachdem Sie eine Zuordnung bearbeitet haben, AWS Systems Manager wird eine neue Version erstellt. Anweisungen zum Bearbeiten einer Zuordnung finden Sie im AWS Systems Manager Benutzerhandbuch unter [Bearbeiten und Erstellen einer neuen Version einer Zuordnung](#).

[SSM.4] SSM-Dokumente sollten nicht öffentlich sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SC-7

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Kritisch

Art der Ressource: AWS : : SSM : : Document

AWS Config -Regel: [ssm-document-not-public](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Mit dieser Kontrolle wird geprüft, ob AWS Systems Manager Dokumente, die dem Konto gehören, öffentlich sind. Diese Kontrolle schlägt fehl, wenn Systems Manager Manager-Dokumente mit dem Eigentümer öffentlich Self sind.

Öffentliche Systems Manager Manager-Dokumente ermöglichen möglicherweise unbeabsichtigten Zugriff auf Ihre Dokumente. Ein öffentliches Systems Manager Manager-Dokument kann wertvolle Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse enthalten.

Sofern Ihr Anwendungsfall die öffentliche Freigabe nicht erfordert, empfehlen wir, die Einstellung für die öffentliche Freigabe für Systems Manager Manager-Dokumente zu blockieren, die Eigentum von sindSelf.

Abhilfe

Informationen zum Blockieren der öffentlichen Freigabe von Systems Manager Manager-Dokumenten finden Sie unter [Blockieren der öffentlichen Freigabe von SSM-Dokumenten](#) im AWS Systems Manager Benutzerhandbuch.

[SSM.5] SSM-Dokumente sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: AWS::SSM::Document

AWS Config -Regel: [ssm-document-tagged](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Eine Liste der Tag-Schlüssel vom Typ „“, die einer ausgewerteten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS Systems Manager Dokument über die im `requiredKeyTags` Parameter angegebenen Tagschlüssel verfügt. Das Steuerelement schlägt fehl, wenn das Dokument keine Tag-Schlüssel oder nicht alle im `requiredKeyTags` Parameter angegebenen Schlüssel hat. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Dokument keine Tagschlüssel hat. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws:` Präfix haben. Die Kontrolle bewertet keine Systems Manager-Dokumente, die Amazon gehören.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen](#)

mit [ABAC-Autorisierung](#) im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im [Tagging AWS Resources and Tag Editor User Guide](#).

 Note

Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Um einem AWS Systems Manager Dokument Tags hinzuzufügen, können Sie den [AddTagsToResource](#) Betrieb der AWS Systems Manager API verwenden oder, falls Sie die verwenden AWS CLI, den [add-tags-to-resource](#) Befehl ausführen. Sie können auch die AWS Systems Manager -Konsole verwenden.

[SSM.6] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS:::Account

AWS Config -Regel: [ssm-automation-logging-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob die CloudWatch Amazon-Protokollierung für AWS Systems Manager (SSM) Automation aktiviert ist. Die Kontrolle schlägt fehl, wenn die CloudWatch Protokollierung für SSM Automation nicht aktiviert ist.

SSM Automation ist ein AWS Systems Manager Tool, mit dem Sie automatisierte Lösungen für die skalierbare Bereitstellung, Konfiguration und Verwaltung von AWS Ressourcen mithilfe vordefinierter oder benutzerdefinierter Runbooks erstellen können. Um die Betriebs- oder Sicherheitsanforderungen für Ihr Unternehmen zu erfüllen, müssen Sie möglicherweise eine Aufzeichnung der ausgeführten Skripts bereitstellen. Sie können SSM Automation so konfigurieren, dass die Ausgabe von `aws:executeScript` Aktionen in Ihren Runbooks an eine von Ihnen

angegebene Amazon CloudWatch Logs-Protokollgruppe gesendet wird. Mit CloudWatch Logs können Sie Protokolldateien aus verschiedenen Quellen überwachen, speichern und darauf zugreifen. AWS-Services

Abhilfe

Informationen zur Aktivierung der CloudWatch Protokollierung für SSM Automation finden Sie unter [Ausgabe der Automatisierungsaktion protokollieren mit CloudWatch Protokollen](#) im AWS Systems Manager Benutzerhandbuch.

[SSM.7] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein

Kategorie: Schützen > Sichere Zugriffsverwaltung > Ressource nicht öffentlich zugänglich

Schweregrad: Kritisch

Art der Ressource: AWS:::Account

AWS Config -Regel: [ssm-automation-block-public-sharing](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob die Einstellung „Öffentliche Freigabe blockieren“ für AWS Systems Manager Dokumente aktiviert ist. Die Steuerung schlägt fehl, wenn die Einstellung Öffentliche Freigabe blockieren für Systems Manager Manager-Dokumente deaktiviert ist.

Die Einstellung „Öffentliches Teilen von Dokumenten blockieren“ AWS Systems Manager (SSM) ist eine Einstellung auf Kontoebene. Durch die Aktivierung dieser Einstellung kann unerwünschter Zugriff auf Ihre SSM-Dokumente verhindert werden. Wenn Sie diese Einstellung aktivieren, wirkt sich Ihre Änderung nicht auf SSM-Dokumente aus, die Sie derzeit für die Öffentlichkeit freigeben. Sofern Ihr Anwendungsfall nicht erfordert, dass Sie SSM-Dokumente für die Öffentlichkeit freigeben, empfehlen wir Ihnen, die Einstellung „Öffentliches Teilen blockieren“ zu aktivieren. Die Einstellung kann für jede AWS-Region Einstellung unterschiedlich sein.

Abhilfe

Informationen zur Aktivierung der Einstellung „Öffentliches Teilen blockieren“ für Dokumente AWS Systems Manager (SSM) finden Sie im AWS Systems Manager Benutzerhandbuch unter [Öffentliche Freigabe für SSM-Dokumente blockieren](#).

Security Hub-Steuerungen für AWS Transfer Family

Diese AWS Security Hub Kontrollen bewerten den AWS Transfer Family Service und die Ressourcen. Die Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[Transfer.1] AWS Transfer Family -Workflows sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Transfer::Workflow`

AWS Config Regel: `tagged-transfer-workflow` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredTagKeys</code>	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	No default value

Dieses Steuerelement prüft, ob ein AWS Transfer Family Workflow Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn der Workflow keine Tagschlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält `requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Workflow mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit `beginnenaws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter [Wozu dient ABAC?](#) AWS im IAM-Benutzerhandbuch.

 Note

Fügen Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

Abhilfe

So fügen Sie Stichwörter zu einem Transfer Family Family-Workflow hinzu (Konsole)

1. Öffnen Sie die AWS Transfer Family Konsole.
2. Wählen Sie im Navigationsbereich die Option Workflows aus. Wählen Sie dann den Workflow aus, den Sie taggen möchten.
3. Wählen Sie Tags verwalten aus und fügen Sie dann die Tags hinzu.

[Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden

Verwandte Anforderungen: NIST.800-53.r5 CM-7, NIST.800-53.r5 IA-5,, PCI DSS NIST.800-53.r5 SC-8 v4.0.1/4.2.1

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: AWS::Transfer::Server

AWS Config -Regel: [transfer-family-server-no-ftp](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein AWS Transfer Family Server ein anderes Protokoll als FTP für die Endpunktverbindung verwendet. Die Steuerung schlägt fehl, wenn der Server das FTP-Protokoll verwendet, damit ein Client eine Verbindung zum Serverendpunkt herstellt.

FTP (File Transfer Protocol) stellt die Endpunktverbindung über unverschlüsselte Kanäle her, sodass Daten, die über diese Kanäle gesendet werden, abgefangen werden können. Die Verwendung von SFTP (SSH File Transfer Protocol), FTPS (File Transfer Protocol Secure) oder AS2 (Applicability Statement 2) bietet eine zusätzliche Sicherheitsebene, indem Ihre Daten während der Übertragung verschlüsselt werden, und kann dazu verwendet werden, potenzielle Angreifer daran zu hindern, den Netzwerkverkehr zu belauschen person-in-the-middle oder zu manipulieren.

Abhilfe

Informationen zum Ändern des Protokolls für einen Transfer Family Family-Server finden Sie unter [Bearbeiten der Dateiübertragungsprotokolle](#) im AWS Transfer Family Benutzerhandbuch.

[Transfer.3] Bei Connectoren der Transfer-Familie sollte die Protokollierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-2 (12), (4), NIST.800-53.r5 AC-2 (26), (9), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 NIST.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-9(7), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-4, NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Ressourcentyp: AWS::Transfer::Connector

AWS Config -Regel: [transfer-connector-logging-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die CloudWatch Amazon-Protokollierung für einen AWS Transfer Family Connector aktiviert ist. Die Steuerung schlägt fehl, wenn die CloudWatch Protokollierung für den Connector nicht aktiviert ist.

Amazon CloudWatch ist ein Überwachungs- und Beobachtbarkeitsservice, der Einblick in Ihre AWS Ressourcen, einschließlich AWS Transfer Family Ressourcen, bietet. Für Transfer Family CloudWatch bietet eine konsolidierte Prüfung und Protokollierung des Workflow-Fortschritts und der Ergebnisse. Dazu gehören mehrere Metriken, die Transfer Family für Workflows definiert. Sie können Transfer Family so konfigurieren, dass Connector-Ereignisse automatisch protokolliert CloudWatch werden. Dazu geben Sie eine Protokollierungsrolle für den Connector an. Für die Protokollierungsrolle erstellen Sie eine IAM-Rolle und eine ressourcenbasierte IAM-Richtlinie, die die Berechtigungen für die Rolle definiert.

Abhilfe

Informationen zur Aktivierung der CloudWatch Protokollierung für einen Transfer Family Family-Connector finden Sie unter [CloudWatch Amazon-Protokollierung für AWS Transfer Family Server](#) im AWS Transfer Family Benutzerhandbuch.

[Transfer.4] Transfer Family Familienverträge sollten gekennzeichnet werden

Kategorie: Identifizieren > Inventar > Kennzeichnung

Schweregrad: Niedrig

Art der Ressource: AWS::Transfer::Agreement

AWS Config -Regel: [transfer-agreement-tagged](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Eine Liste der Tag-Schlüssel vom Typ „“, die einer ausgewerteten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS Transfer Family Vereinbarung die durch den `requiredKeyTags` Parameter angegebenen Tag-Schlüssel enthält. Das Steuerelement schlägt fehl, wenn die Vereinbarung keine Tagschlüssel oder nicht alle durch den `requiredKeyTags` Parameter angegebenen Schlüssel enthält. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Vereinbarung keine Tagschlüssel enthält. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws:` Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im [Tagging AWS Resources and Tag](#) Editor User Guide.

Note

Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS Transfer Family Vereinbarung finden Sie unter [Methoden zur Kennzeichnung von Ressourcen für Ressourcen und Tag-Editor](#) im Benutzerhandbuch zur Kennzeichnung von AWS Ressourcen und Tag-Editor.

[Transfer.5] Transfer Family Familienzertifikate sollten gekennzeichnet sein

Kategorie: Identifizieren > Inventar > Kennzeichnung

Schweregrad: Niedrig

Art der Ressource: `AWS::Transfer::Certificate`

AWS Config -Regel: [transfer-certificate-tagged](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Eine Liste der Tag-Schlüssel vom Typ „“, die einer ausgewerteten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS Transfer Family Zertifikat über die im `requiredKeyTags` Parameter angegebenen Tagschlüssel verfügt. Die Steuerung schlägt fehl, wenn das Zertifikat keine Tagschlüssel oder nicht alle im `requiredKeyTags` Parameter angegebenen Schlüssel enthält. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Zertifikat keine Tagschlüssel enthält. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws:` Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im [Tagging AWS Resources and Tag Editor User Guide](#).

Note

Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS Transfer Family Zertifikat finden Sie unter [Methoden zur Kennzeichnung von Ressourcen für Ressourcen und Tag-Editor](#) im Benutzerhandbuch zur Kennzeichnung von AWS Ressourcen und Tag-Editor.

[Transfer.6] Steckverbinder der Transfer-Familie sollten gekennzeichnet sein

Kategorie: Identifizieren > Inventar > Kennzeichnung

Schweregrad: Niedrig

Art der Ressource: `AWS::Transfer::Connector`

AWS Config -Regel: [transfer-connector-tagged](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Eine Liste der Tag-Schlüssel vom Typ „“, die einer ausgewerteten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS Transfer Family Konnektor über die im `requiredKeyTags` Parameter angegebenen Tag-Schlüssel verfügt. Das Steuerelement schlägt fehl, wenn der Konnektor keine Tag-Schlüssel oder nicht alle im `requiredKeyTags` Parameter angegebenen Schlüssel hat. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Konnektor keine Tag-Schlüssel hat. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws:` Präfix haben.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im [Tagging AWS Resources and Tag](#) Editor User Guide.

Note

Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS Transfer Family Connector finden Sie unter [Methoden zur Kennzeichnung von Ressourcen](#) für AWS Ressourcen und Tag-Editor für Ressourcen mit Tags.

[Transfer.7] Familienprofile sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Kennzeichnung

Schweregrad: Niedrig

Art der Ressource: `AWS::Transfer::Profile`

AWS Config -Regel: [transfer-profile-tagged](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
<code>requiredKeyTags</code>	Eine Liste der Tag-Schlüssel vom Typ „“, die einer ausgewerteten Ressource zugewiesen werden müssen. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList (maximal 6 Elemente)	1—6 Tag-Schlüssel, die die AWS Anforderungen erfüllen.	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS Transfer Family Profil die durch den `requiredKeyTags` Parameter angegebenen Tag-Schlüssel enthält. Das Steuerelement schlägt fehl, wenn das Profil keine Tagschlüssel oder nicht alle im `requiredKeyTags` Parameter angegebenen Schlüssel hat. Wenn Sie keine Werte für den `requiredKeyTags` Parameter angeben, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Profil keine Tagschlüssel hat. Das Steuerelement ignoriert Systemtags, die automatisch angewendet werden und das `aws :` Präfix haben. Das Steuerelement wertet lokale Profile und Partnerprofile aus.

Ein Tag ist eine Bezeichnung, die Sie erstellen und einer AWS Ressource zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Sie können Ihnen helfen, Ressourcen zu identifizieren, zu organisieren, zu suchen und zu filtern. Sie können Ihnen auch dabei helfen, Ressourcenbesitzer im Hinblick auf Aktionen und Benachrichtigungen zu verfolgen. Sie können Tags auch verwenden, um die attributbasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie zu implementieren. Weitere Informationen zu ABAC-Strategien finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch. Weitere Informationen zu Tags finden Sie im [Tagging AWS Resources and Tag Editor User Guide](#).

Note

Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Auf Tags kann von vielen AWS-Services aus zugegriffen werden. Sie sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Abhilfe

Informationen zum Hinzufügen von Stichwörtern zu einem AWS Transfer Family Profil finden Sie unter [Methoden zur Kennzeichnung von Ressourcen](#) für AWS Ressourcen und Tag-Editor.

Security Hub Hub-Kontrollen für AWS WAF

Diese AWS Security Hub Kontrollen bewerten den AWS WAF Service und die Ressourcen. Die Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (26), (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-7 NIST.800-53.r5 SC-7 (8), PCI DSS v4.0.1/10.4.2

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS::WAF::WebACL

AWS Config -Regel: [waf-classic-logging-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob die Protokollierung für eine AWS WAF globale Web-ACL aktiviert ist. Diese Steuerung schlägt fehl, wenn die Protokollierung für die Web-ACL nicht aktiviert ist.

Protokollierung ist ein wichtiger Teil der Aufrechterhaltung von Zuverlässigkeit, Verfügbarkeit und Performance von AWS WAF global. Sie ist in vielen Unternehmen eine Geschäfts- und Compliance-Anforderung und ermöglicht es Ihnen, Fehler beim Verhalten von Anwendungen zu beheben. Es enthält auch detaillierte Informationen über den Datenverkehr, der von der Web-ACL analysiert wird, die angehängt ist AWS WAF.

Abhilfe

Informationen zum Aktivieren der Protokollierung für eine AWS WAF Web-ACL finden Sie unter [Logging Web-ACL-Verkehrsinformationen](#) im AWS WAF Developer Guide.

[WAF.2] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung haben

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21)

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: AWS::WAFRegional::Rule

AWS Config -Regel: [waf-regional-rule-not-empty](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine AWS WAF Regionalregel mindestens eine Bedingung hat. Die Steuerung schlägt fehl, wenn in einer Regel keine Bedingungen vorhanden sind.

Eine regionale WAF-Regel kann mehrere Bedingungen enthalten. Die Bedingungen der Regel ermöglichen eine Verkehrsprüfung und eine definierte Aktion (Zulassen, Blockieren oder Zählen). Wenn keine Bedingungen erfüllt sind, wird der Verkehr ohne Inspektion weitergeleitet. Eine WAF-Regionalregel ohne Bedingungen, aber mit einem Namen oder Tag, der auf Zulassen, Blockieren oder Zählen hindeutet, könnte zu der falschen Annahme führen, dass eine dieser Aktionen stattfindet.

Abhilfe

Informationen zum Hinzufügen einer Bedingung zu einer leeren Regel finden Sie unter [Hinzufügen und Entfernen von Bedingungen in einer Regel](#) im AWS WAF Entwicklerhandbuch.

[WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21)

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: AWS::WAFRegional::RuleGroup

AWS Config -Regel: [waf-regional-rulegroup-not-empty](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine AWS WAF regionale Regelgruppe mindestens eine Regel hat. Die Steuerung schlägt fehl, wenn innerhalb einer Regelgruppe keine Regeln vorhanden sind.

Eine regionale WAF-Regelgruppe kann mehrere Regeln enthalten. Die Bedingungen der Regel ermöglichen eine Verkehrsprüfung und eine definierte Aktion (Zulassen, Blockieren oder Zählen). Ohne Regeln passiert der Verkehr ohne Inspektion. Eine regionale WAF-Regelgruppe ohne Regeln, aber mit einem Namen oder Tag, der auf Zulassen, Blockieren oder Zählen hindeutet, könnte zu der falschen Annahme führen, dass eine dieser Aktionen stattfindet.

Abhilfe

Informationen zum Hinzufügen von Regeln und Regelbedingungen zu einer leeren Regelgruppe finden Sie unter [Hinzufügen und Löschen von Regeln aus einer AWS WAF klassischen Regelgruppe](#) und [Hinzufügen und Entfernen von Bedingungen in einer Regel](#) im AWS WAF Entwicklerhandbuch.

[WAF.4] AWS WAF Classic Regional Web ACLs sollte mindestens eine Regel oder Regelgruppe enthalten

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: AWS::WAFRegional::WebACL

AWS Config -Regel: [waf-regional-webacl-not-empty](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Kontrollen überprüft, ob eine AWS WAF Classic Regional Web-ACL WAF-Regeln oder WAF-Regelgruppen enthält. Diese Steuerung schlägt fehl, wenn eine Web-ACL keine WAF-Regeln oder -Regelgruppen enthält.

Eine regionale WAF-Web-ACL kann eine Sammlung von Regeln und Regelgruppen enthalten, die Webanforderungen überprüfen und kontrollieren. Wenn eine Web-ACL leer ist, kann der Webdatenverkehr weitergeleitet werden, ohne von WAF erkannt oder bearbeitet zu werden, abhängig von der Standardaktion.

Abhilfe

Informationen zum Hinzufügen von Regeln oder Regelgruppen zu einer leeren AWS WAF Classic Regional Web-ACL finden Sie unter [Bearbeiten einer Web-ACL](#) im AWS WAF Entwicklerhandbuch.

[WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: AWS::WAF::Rule

AWS Config -Regel: [waf-global-rule-not-empty](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Kontrollen überprüft, ob eine AWS WAF globale Regel Bedingungen enthält. Die Steuerung schlägt fehl, wenn in einer Regel keine Bedingungen vorhanden sind.

Eine globale WAF-Regel kann mehrere Bedingungen enthalten. Die Bedingungen einer Regel ermöglichen eine Verkehrsprüfung und eine definierte Aktion (Zulassen, Blockieren oder Zählen). Ohne jegliche Bedingungen wird der Verkehr ohne Inspektion weitergeleitet. Eine globale WAF-Regel ohne Bedingungen, aber mit einem Namen oder Tag, der auf Zulassen, Blockieren oder Zählen hindeutet, könnte zu der falschen Annahme führen, dass eine dieser Aktionen stattfindet.

Abhilfe

Anweisungen zum Erstellen einer Regel und zum Hinzufügen von Bedingungen finden Sie unter [Regel erstellen und Bedingungen hinzufügen](#) im AWS WAF Entwicklerhandbuch.

[WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: AWS::WAF::RuleGroup

AWS Config -Regel: [waf-global-rulegroup-not-empty](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine AWS WAF globale Regelgruppe mindestens eine Regel hat. Die Steuerung schlägt fehl, wenn innerhalb einer Regelgruppe keine Regeln vorhanden sind.

Eine globale WAF-Regelgruppe kann mehrere Regeln enthalten. Die Bedingungen der Regel ermöglichen eine Verkehrsprüfung und eine definierte Aktion (Zulassen, Blockieren oder Zählen). Ohne Regeln passiert der Verkehr ohne Inspektion. Eine globale WAF-Regelgruppe ohne Regeln, aber mit einem Namen oder Tag, der auf Zulassen, Blockieren oder Zählen hindeutet, könnte zu der falschen Annahme führen, dass eine dieser Aktionen stattfindet.

Abhilfe

Anweisungen zum Hinzufügen einer Regel zu einer Regelgruppe finden Sie unter [Creating an AWS WAF Classic Rule Group](#) im AWS WAF Developer Guide.

[WAF.8] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21)

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: AWS::WAF::WebACL

AWS Config -Regel: [waf-global-webacl-not-empty](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine AWS WAF globale Web-ACL mindestens eine WAF-Regel oder WAF-Regelgruppe enthält. Die Steuerung schlägt fehl, wenn eine Web-ACL keine WAF-Regeln oder -Regelgruppen enthält.

Eine globale WAF-Web-ACL kann eine Sammlung von Regeln und Regelgruppen enthalten, die Webanforderungen überprüfen und kontrollieren. Wenn eine Web-ACL leer ist, kann der Webdatenverkehr weitergeleitet werden, ohne von WAF erkannt oder bearbeitet zu werden, abhängig von der Standardaktion.

Abhilfe

Informationen zum Hinzufügen von Regeln oder Regelgruppen zu einer leeren AWS WAF globalen Web-ACL finden Sie unter [Bearbeiten einer Web-ACL](#) im AWS WAF Entwicklerhandbuch. Wählen Sie für Filter die Option Global (CloudFront).

[WAF.10] AWS WAF web ACLs sollte mindestens eine Regel oder Regelgruppe haben

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: AWS::WAFv2::WebACL

AWS Config -Regel: [wafv2-webacl-not-empty](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine AWS WAF V2-Web-Zugriffskontrollliste (Web-ACL) mindestens eine Regel oder Regelgruppe enthält. Die Steuerung schlägt fehl, wenn eine Web-ACL keine Regeln oder Regelgruppen enthält.

Eine Web-ACL ermöglicht eine differenziertere Kontrolle aller HTTP (S) -Webanforderungen, auf die Ihre geschützte Ressource reagiert. Eine Web-ACL sollte eine Sammlung von Regeln und Regelgruppen enthalten, die Webanforderungen überprüfen und kontrollieren. Wenn eine Web-ACL

leer ist, kann der Webdatenverkehr weitergeleitet werden, ohne erkannt oder bearbeitet zu werden, AWS WAF abhängig von der Standardaktion.

Abhilfe

Informationen zum Hinzufügen von Regeln oder Regelgruppen zu einer leeren WAFV2 Web-ACL finden Sie unter [Bearbeiten einer Web-ACL](#) im AWS WAF Entwicklerhandbuch.

[WAF.11] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (26), (10), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-7 NIST.800-53.r5 SC-7 (8), PCI DSS v4.0.1/10.4.2

Kategorie: Identifizieren > Protokollierung

Schweregrad: Niedrig

Art der Ressource: AWS::WAFv2::WebACL

AWS Config Regel: [wafv2-logging-enabled](#)

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle überprüft, ob die Protokollierung für eine AWS WAF V2-Web-Zugriffssteuerungsliste (Web-ACL) aktiviert ist. Diese Kontrolle schlägt fehl, wenn die Protokollierung für die Web-ACL deaktiviert ist.

Note

Dieses Steuerelement überprüft nicht, ob die AWS WAF Web-ACL-Protokollierung für ein Konto über Amazon Security Lake aktiviert ist.

Protokollierung bewahrt die Zuverlässigkeit, Verfügbarkeit und Leistung von AWS WAF. Darüber hinaus ist die Protokollierung in vielen Organisationen eine Geschäfts- und Compliance-Anforderung. Durch die Protokollierung des Datenverkehrs, der von Ihrer Web-ACL analysiert wird, können Sie Fehler beim Verhalten von Anwendungen beheben.

Abhilfe

Informationen zur Aktivierung der Protokollierung für eine AWS WAF Web-ACL finden Sie unter [Verwaltung der Protokollierung für eine Web-ACL](#) im AWS WAF Entwicklerhandbuch.

Für [WAF.12] AWS WAF Regeln sollten Metriken aktiviert sein CloudWatch

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (26), (10), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-7 NIST.800-53.r5 SC-7 (8), NIST.800-171.R2 3.14.6, NIST.800-171.r2 3.14.7

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: AWS::WAFv2::RuleGroup

AWS Config Regel: [wafv2-rulegroup-logging-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für eine AWS WAF Regel oder Regelgruppe CloudWatch Amazon-Metriken aktiviert sind. Die Kontrolle schlägt fehl, wenn für die Regel oder Regelgruppe keine CloudWatch Metriken aktiviert sind.

Durch die Konfiguration von CloudWatch Metriken AWS WAF für Regeln und Regelgruppen erhalten Sie Einblick in den Verkehrsfluss. Sie können sehen, welche ACL-Regeln ausgelöst werden und welche Anfragen akzeptiert und blockiert werden. Diese Sichtbarkeit kann Ihnen helfen, böswillige Aktivitäten auf Ihren verknüpften Ressourcen zu erkennen.

Abhilfe

Rufen Sie die [UpdateRuleGroup](#)API auf, um CloudWatch Metriken für eine AWS WAF Regelgruppe zu aktivieren. Rufen Sie die [UpdateWebACL-API](#) auf, um CloudWatch Metriken für eine AWS WAF Regel zu aktivieren. Stellen Sie das CloudWatchMetricsEnabled Feld auf ein. true Wenn Sie die AWS WAF Konsole verwenden, um Regeln oder Regelgruppen zu erstellen, werden CloudWatch Metriken automatisch aktiviert.

Security Hub-Steuerungen für WorkSpaces

Diese AWS Security Hub Kontrollen bewerten den WorkSpaces Service und die Ressourcen von Amazon.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

[WorkSpaces.1] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: AWS::WorkSpaces::Workspace

AWS Config -Regel: [workspaces-user-volume-encryption-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Benutzervolume in einem Amazon im Ruhezustand verschlüsselt WorkSpaces Workspace ist. Die Kontrolle schlägt fehl, wenn das Workspace Benutzervolume im Ruhezustand nicht verschlüsselt ist.

Daten im Ruhezustand beziehen sich auf Daten, die für einen beliebigen Zeitraum in einem persistenten, nichtflüchtigen Speicher gespeichert werden. Durch die Verschlüsselung ruhender Daten können Sie deren Vertraulichkeit schützen, wodurch das Risiko verringert wird, dass ein nicht autorisierter Benutzer darauf zugreifen kann.

Abhilfe

Informationen zum Verschlüsseln eines WorkSpaces Benutzervolumes finden Sie unter [Encrypt a Workspace](#) im WorkSpaces Amazon-Administratorhandbuch.

[WorkSpaces.2] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: AWS::WorkSpaces::Workspace

AWS Config -Regel: [workspaces-root-volume-encryption-enabled](#)

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Root-Volume in einem Amazon im Ruhezustand verschlüsselt WorkSpaces Workspace ist. Die Kontrolle schlägt fehl, wenn das Workspace Root-Volume im Ruhezustand nicht verschlüsselt ist.

Daten im Ruhezustand beziehen sich auf Daten, die für einen beliebigen Zeitraum in einem persistenten, nichtflüchtigen Speicher gespeichert werden. Durch die Verschlüsselung ruhender Daten können Sie deren Vertraulichkeit schützen, wodurch das Risiko verringert wird, dass ein nicht autorisierter Benutzer darauf zugreifen kann.

Abhilfe

Informationen zum Verschlüsseln eines WorkSpaces Root-Volumes finden Sie unter [Encrypt a Workspace](#) im WorkSpaces Amazon-Administratorhandbuch.

Erforderliche Berechtigungen zur Konfiguration von Steuerelementen in Security Hub CSPM

Um Informationen über Sicherheitskontrollen anzuzeigen und Sicherheitskontrollen in Standards zu aktivieren und zu deaktivieren, benötigt die AWS Identity and Access Management (IAM) -Rolle, die Sie für den Zugriff auf AWS Security Hub Cloud Security Posture Management (CSPM) verwenden, Berechtigungen, um die folgenden Operationen der Security Hub CSPM-API aufzurufen.

Um die erforderlichen Berechtigungen zu erhalten, können Sie [verwaltete Security Hub CSPM-Richtlinien](#) verwenden. Alternativ können Sie benutzerdefinierte IAM-Richtlinien so aktualisieren, dass sie auch Berechtigungen für diese Aktionen enthalten.

- [BatchGetSecurityControls](#)— Gibt Informationen zu einer Reihe von Sicherheitskontrollen für das Girokonto zurück und AWS-Region.
- [ListSecurityControlDefinitions](#)— Gibt Informationen über Sicherheitskontrollen zurück, die für einen bestimmten Standard gelten.
- [ListStandardsControlAssociations](#)— Identifiziert, ob eine Sicherheitskontrolle derzeit in jedem aktivierten Standard im Konto aktiviert oder deaktiviert ist.

- [BatchGetStandardsControlAssociations](#)— Identifiziert für eine Reihe von Sicherheitskontrollen, ob die einzelnen Kontrollen derzeit in einem bestimmten Standard aktiviert oder deaktiviert sind.
- [BatchUpdateStandardsControlAssociations](#)— Wird verwendet, um eine Sicherheitskontrolle in Standards zu aktivieren, die die Steuerung beinhalten, oder um eine Steuerung in Standards zu deaktivieren. Dies ist ein Batch-Ersatz für den bestehenden [UpdateStandardsControl](#)Vorgang.
- [BatchUpdateStandardsControlAssociations](#)— Wird verwendet, um eine Reihe von Sicherheitskontrollen in Standards zu aktivieren oder zu deaktivieren, die diese Kontrollen enthalten. Dies ist ein Batch-Ersatz für den bestehenden [UpdateStandardsControl](#)Vorgang.
- [UpdateStandardsControl](#)— Wird verwendet, um eine einzelne Sicherheitskontrolle in Standards zu aktivieren oder zu deaktivieren, die die Steuerung beinhalten
- [DescribeStandardsControl](#)— Gibt Details zu den angegebenen Sicherheitskontrollen zurück.

Zusätzlich zu den oben genannten Informationen APIs sollten Sie Ihrer IAM-Rolle die Berechtigung `BatchGetControlEvaluations` zum Anrufen hinzufügen. Diese Berechtigung ist erforderlich, um den Aktivierungs- und Konformitätsstatus einer Kontrolle, die Ergebnisse für eine Kontrolle und die Gesamtsicherheitsbewertung für Kontrollen auf der Security Hub CSPM-Konsole einzusehen. Da nur die Konsole aufruft `BatchGetControlEvaluations`, entspricht diese Berechtigung nicht direkt den öffentlich dokumentierten Security Hub CSPM APIs oder AWS CLI Befehlen.

Steuerelemente in Security Hub CSPM aktivieren

In AWS Security Hub Cloud Security Posture Management (CSPM) ist eine Kontrolle eine Schutzmaßnahme innerhalb eines Sicherheitsstandards, die einem Unternehmen hilft, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationen zu schützen. Jedes Security Hub CSPM-Steuerelement bezieht sich auf eine bestimmte AWS Ressource. Wenn Sie ein Steuerelement aktivieren, beginnt Security Hub CSPM mit der Durchführung von Sicherheitsprüfungen für das Steuerelement und generiert Ergebnisse dafür. Security Hub CSPM berücksichtigt bei der Berechnung der Sicherheitsbewertungen auch alle aktivierten Kontrollen.

Sie können sich dafür entscheiden, eine Kontrolle für alle Sicherheitsstandards zu aktivieren, für die sie gilt. Alternativ können Sie den Aktivierungsstatus in verschiedenen Standards unterschiedlich konfigurieren. Wir empfehlen die erstere Option, bei der der Aktivierungsstatus einer Steuerung auf alle aktivierten Standards abgestimmt ist. Anweisungen zur Aktivierung eines Steuerelements für alle Standards, auf die es angewendet wird, finden Sie unter [Aktivierung einer standardübergreifenden Steuerung](#). Anweisungen zur Aktivierung eines Steuerelements in bestimmten Standards finden Sie unter [Aktivierung einer Steuerung in einem bestimmten Standard](#).

Wenn Sie die regionsübergreifende Aggregation aktivieren und sich bei einer Aggregationsregion anmelden, zeigt die Security Hub CSPM-Konsole Steuerelemente an, die in mindestens einer verknüpften Region verfügbar sind. Wenn ein Steuerelement in einer verknüpften Region verfügbar ist, aber nicht in der Aggregationsregion, können Sie dieses Steuerelement nicht in der Aggregationsregion aktivieren oder deaktivieren.

Sie können Steuerungen in jeder Region aktivieren und deaktivieren, indem Sie die Security Hub CSPM-Konsole, die Security Hub CSPM-API oder verwenden. AWS CLI

[Die Anweisungen zum Aktivieren und Deaktivieren von Steuerungen variieren je nachdem, ob Sie die zentrale Konfiguration verwenden oder nicht.](#) In diesem Thema werden die Unterschiede beschrieben. Die zentrale Konfiguration steht Benutzern zur Verfügung, die Security Hub CSPM und integrieren. AWS Organizations Wir empfehlen, die zentrale Konfiguration zu verwenden, um das Aktivieren und Deaktivieren von Steuerungen in Umgebungen mit mehreren Konten und mehreren Regionen zu vereinfachen. Wenn Sie die zentrale Konfiguration verwenden, können Sie mithilfe von Konfigurationsrichtlinien eine Steuerung über mehrere Konten und Regionen hinweg aktivieren. Wenn Sie die zentrale Konfiguration nicht verwenden, müssen Sie eine Steuerung für jede Region und jedes Konto separat aktivieren.

Aktivierung einer standardübergreifenden Steuerung

Wir empfehlen, eine AWS Security Hub Cloud Security Posture Management (CSPM) -Steuerung für alle Standards zu aktivieren, für die die Kontrolle gilt. Wenn Sie konsolidierte Kontrollergebnisse aktivieren, erhalten Sie ein Ergebnis pro Kontrollprüfung, auch wenn eine Kontrolle zu mehr als einem Standard gehört.

Standardübergreifende Aktivierung in Umgebungen mit mehreren Konten und mehreren Regionen

[Um eine Sicherheitskontrolle über mehrere AWS-Konten und zu aktivieren AWS-Regionen, müssen Sie mit dem delegierten Security Hub CSPM-Administratorkonto angemeldet sein und die zentrale Konfiguration verwenden.](#)

Bei der zentralen Konfiguration kann der delegierte Administrator Security Hub CSPM-Konfigurationsrichtlinien erstellen, die bestimmte Kontrollen für alle aktivierten Standards ermöglichen. Anschließend können Sie die Konfigurationsrichtlinie bestimmten Konten und Organisationseinheiten (OUs) oder dem Stamm zuordnen. Eine Konfigurationsrichtlinie wird in Ihrer Heimatregion (auch Aggregationsregion genannt) und allen verknüpften Regionen wirksam.

Konfigurationsrichtlinien bieten Anpassungsmöglichkeiten. Sie können beispielsweise festlegen, dass alle Steuerelemente in einer Organisationseinheit aktiviert werden, und Sie können festlegen, dass nur Amazon Elastic Compute Cloud (EC2) -Steuerelemente in einer anderen Organisationseinheit aktiviert werden. Der Grad der Granularität hängt von Ihren angestrebten Zielen für die Sicherheitsabdeckung in Ihrem Unternehmen ab. Anweisungen zum Erstellen einer Konfigurationsrichtlinie, die bestimmte Standardkontrollen ermöglicht, finden Sie unter [Konfigurationsrichtlinien erstellen und zuordnen](#).

 Note

Der delegierte Administrator kann Konfigurationsrichtlinien erstellen, um Kontrollen in allen Standards außer dem [Service-Managed Standard](#) zu verwalten. AWS Control Tower Die Kontrollen für diesen Standard sollten im Service konfiguriert werden. AWS Control Tower

Wenn Sie möchten, dass einige Konten ihre eigenen Steuerungen konfigurieren und nicht der delegierte Administrator, kann der delegierte Administrator diese Konten als selbstverwaltet kennzeichnen. Selbstverwaltete Konten müssen die Kontrollen in jeder Region separat konfigurieren.

Standardübergreifende Aktivierung für ein einziges Konto und eine Region

Wenn Sie keine zentrale Konfiguration verwenden oder ein selbstverwaltetes Konto haben, können Sie keine Konfigurationsrichtlinien verwenden, um Steuerungen in mehreren Konten und Regionen zentral zu aktivieren. Sie können jedoch die folgenden Schritte verwenden, um eine Steuerung für ein einzelnes Konto und eine Region zu aktivieren.

Security Hub CSPM console

Um eine standardübergreifende Steuerung in einem Konto und einer Region zu ermöglichen

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Controls aus.
3. Wählen Sie die Registerkarte Deaktiviert.
4. Wählen Sie die Option neben einem Steuerelement aus.
5. Wählen Sie Steuerung aktivieren (diese Option wird nicht für ein Steuerelement angezeigt, das bereits aktiviert ist).

6. Wiederholen Sie den Vorgang in jeder Region, in der Sie das Steuerelement aktivieren möchten.

Security Hub CSPM API

Um eine standardübergreifende Steuerung in einem Konto und einer Region zu ermöglichen

1. Rufen Sie die [ListStandardsControlAssociations](#)API auf. Geben Sie eine Sicherheitskontroll-ID an.

Beispiel für eine Anfrage:

```
{
  "SecurityControlId": "IAM.1"
}
```

2. Rufen Sie die [BatchUpdateStandardsControlAssociations](#)API auf. Geben Sie den Amazon-Ressourcennamen (ARN) aller Standards an, in denen die Steuerung nicht aktiviert ist. Führen Sie den Befehl aus ARNs, um den Standard abzurufen [DescribeStandards](#).
3. Stellen Sie den AssociationStatus Parameter aufENABLED. Wenn Sie diese Schritte für ein Steuerelement ausführen, das bereits aktiviert ist, gibt die API eine Antwort mit dem HTTP-Statuscode 200 zurück.

Beispiel für eine Anfrage:

```
{
  "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub::standards/aws-foundational-security-best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]
}
```

4. Wiederholen Sie dies in jeder Region, in der Sie das Steuerelement aktivieren möchten.

AWS CLI

Um eine standardübergreifende Steuerung in einem Konto und einer Region zu ermöglichen

1. Führen Sie den Befehl [list-standards-control-associations](#) aus. Geben Sie eine ID für die Sicherheitskontrolle ein.

```
aws securityhub --region us-east-1 list-standards-control-associations --  
security-control-id CloudTrail.1
```

2. Führen Sie den Befehl [batch-update-standards-control-associations](#) aus. Geben Sie den Amazon-Ressourcennamen (ARN) aller Standards an, in denen die Steuerung nicht aktiviert ist. Um den Standard zu erhalten ARNs, führen Sie den `describe-standards` Befehl aus.
3. Stellen Sie den `AssociationStatus` Parameter auf `ENABLED`. Wenn Sie diese Schritte für ein Steuerelement ausführen, das bereits aktiviert ist, gibt der Befehl eine Antwort mit dem HTTP-Statuscode 200 zurück.

```
aws securityhub --region us-east-1 batch-update-standards-control-associations  
--standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",  
"StandardsArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/  
v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "CloudTrail.1",  
"StandardsArn": "arn:aws:securityhub::standards/cis-aws-foundations-benchmark/  
v/1.4.0", "AssociationStatus": "ENABLED"}]'
```

4. Wiederholen Sie den Vorgang in jeder Region, in der Sie das Steuerelement aktivieren möchten.

Aktivierung einer Steuerung in einem bestimmten Standard

Wenn Sie einen Standard in AWS Security Hub Cloud Security Posture Management (CSPM) aktivieren, werden alle Kontrollen, die für ihn gelten, automatisch in diesem Standard aktiviert (die Ausnahme bilden serviceverwaltete Standards). Anschließend können Sie bestimmte Kontrollen im Standard deaktivieren und wieder aktivieren. Wir empfehlen jedoch, den Aktivierungsstatus eines Steuerelements auf alle aktivierten Standards abzustimmen. Anweisungen zur Aktivierung einer Steuerung für alle Standards finden Sie unter [Aktivierung einer standardübergreifenden Steuerung](#)

Die Detailseite für einen Standard enthält die Liste der für den Standard geltenden Kontrollen sowie Informationen darüber, welche Steuerelemente derzeit in diesem Standard aktiviert und deaktiviert sind.

Auf der Seite mit den Standarddetails können Sie auch Steuerelemente in bestimmten Standards aktivieren. Sie müssen Steuerungen in bestimmten Standards in jedem AWS-Konto Land separat aktivieren AWS-Region. Wenn Sie eine Steuerung in bestimmten Standards aktivieren, wirkt sich dies nur auf die Leistungsbilanz und die Region aus.

Um ein Steuerelement in einem Standard zu aktivieren, müssen Sie zunächst mindestens einen Standard aktivieren, für den das Steuerelement gilt. Anweisungen zur Aktivierung eines Standards finden Sie unter [Einen Sicherheitsstandard aktivieren](#). Wenn Sie eine Kontrolle in einem oder mehreren Standards aktivieren, beginnt Security Hub CSPM, Ergebnisse für diese Kontrolle zu generieren. Security Hub CSPM bezieht den [Kontrollstatus](#) in die Berechnung der Gesamtsicherheitsbewertung und der Standardsicherheitsbewertungen ein. Selbst wenn Sie eine Kontrolle in mehreren Standards aktivieren, erhalten Sie bei jeder standardübergreifenden Sicherheitsüberprüfung ein einziges Ergebnis, wenn Sie die konsolidierten Kontrollergebnisse aktivieren. Weitere Informationen finden Sie unter [Konsolidierte Erkenntnisse zu Kontrollen](#).

Um eine Kontrolle in einem Standard zu aktivieren, muss die Kontrolle in Ihrer aktuellen Region verfügbar sein. Weitere Informationen finden Sie unter [Verfügbarkeit von Steuerelementen nach Regionen](#).

Gehen Sie wie folgt vor, um eine Security Hub CSPM-Steuerung in einem bestimmten Standard zu aktivieren. Anstatt der folgenden Schritte können Sie auch die [UpdateStandardsControl](#) API-Aktion verwenden, um Kontrollen in einem bestimmten Standard zu aktivieren. Anweisungen zur Aktivierung eines Steuerelements in allen Standards finden Sie unter [Standardübergreifende Aktivierung für ein einziges Konto und eine Region](#).

Security Hub CSPM console

So aktivieren Sie ein Steuerelement in einem bestimmten Standard

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Sicherheitsstandards aus.
3. Wählen Sie Ergebnisse anzeigen für den entsprechenden Standard aus.
4. Wählen Sie ein Steuerelement aus.

5. Wählen Sie Steuerung aktivieren (diese Option wird nicht für ein Steuerelement angezeigt, das bereits aktiviert ist). Bestätigen Sie, indem Sie „Aktivieren“ wählen.

Security Hub CSPM API

Um ein Steuerelement in einem bestimmten Standard zu aktivieren

1. Führen Sie [ListSecurityControlDefinitions](#) einen Standard-ARN aus und geben Sie ihn an, um eine Liste der verfügbaren Steuerelemente für einen bestimmten Standard abzurufen. Führen Sie den Befehl aus, um einen Standard-ARN zu erhalten [DescribeStandards](#). Diese API gibt eine standardunabhängige Sicherheitskontrolle zurück IDs, keine standardspezifische Steuerung. IDs

Beispiel für eine Anfrage:

```
{
  "StandardsArn": "arn:aws:securityhub::standards/aws-foundational-security-
  best-practices/v/1.0.0"
}
```

2. Führen Sie [ListStandardsControlAssociations](#) den Vorgang aus und geben Sie eine spezifische Kontroll-ID an, um den aktuellen Aktivierungsstatus eines Steuerelements in jedem Standard zurückzugeben.

Beispiel für eine Anfrage:

```
{
  "SecurityControlId": "IAM.1"
}
```

3. Führen Sie [BatchUpdateStandardsControlAssociations](#). Geben Sie den ARN des Standards an, in dem Sie das Steuerelement aktivieren möchten.
4. Stellen Sie den AssociationStatus Parameter aufENABLED.

Beispiel für eine Anfrage:

```
{
  "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
  "StandardsArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/
  v/1.2.0", "AssociationStatus": "ENABLED"}]
```

```
}
```

AWS CLI

Um ein Steuerelement in einem bestimmten Standard zu aktivieren

1. Führen Sie den [list-security-control-definitions](#) Befehl aus und geben Sie einen Standard-ARN an, um eine Liste der verfügbaren Steuerelemente für einen bestimmten Standard abzurufen. Führen Sie den Befehl aus, um einen Standard-ARN zu erhalten `describe-standards`. Dieser Befehl gibt eine standardunabhängige Sicherheitskontrolle zurück IDs, keine standardspezifische Steuerung. IDs

```
aws securityhub --region us-east-1 list-security-control-definitions --  
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-  
security-best-practices/v/1.0.0"
```

2. Führen Sie den [list-standards-control-associations](#) Befehl aus und geben Sie eine spezifische Kontroll-ID an, um den aktuellen Aktivierungsstatus eines Steuerelements in jedem Standard zurückzugeben.

```
aws securityhub --region us-east-1 list-standards-control-associations --  
security-control-id CloudTrail.1
```

3. Führen Sie den Befehl [batch-update-standards-control-associations](#) aus. Geben Sie den ARN des Standards an, in dem Sie das Steuerelement aktivieren möchten.
4. Stellen Sie den `AssociationStatus` Parameter auf `ENABLED`.

```
aws securityhub --region us-east-1 batch-update-standards-control-associations  
--standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",  
"StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-foundational-  
security-best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]'
```

Automatische Aktivierung neuer Steuerungen in aktivierten Standards

AWS Security Hub Cloud Security Posture Management (CSPM) veröffentlicht regelmäßig neue Kontrollen und fügt sie einem oder mehreren Standards hinzu. Sie können wählen, ob neue Kontrollen in Ihren aktivierten Standards automatisch aktiviert werden sollen.

Wir empfehlen, die zentrale Security Hub CSPM-Konfiguration zu verwenden, um neue Sicherheitskontrollen automatisch zu aktivieren. Sie können Konfigurationsrichtlinien erstellen, die eine Liste von Kontrollen enthalten, die standardübergreifend deaktiviert werden sollen. Alle anderen Steuerelemente, einschließlich der neu veröffentlichten, sind standardmäßig aktiviert. Alternativ können Sie Richtlinien erstellen, die eine Liste von Kontrollen enthalten, die standardübergreifend aktiviert werden sollen. Alle anderen Kontrollen, einschließlich der neu veröffentlichten, sind standardmäßig deaktiviert. Weitere Informationen finden Sie unter [Grundlegendes zur zentralen Konfiguration in Security Hub CSPM](#).

Security Hub CSPM aktiviert keine neuen Steuerelemente, wenn sie zu einem Standard hinzugefügt werden, den Sie nicht aktiviert haben.

Die folgenden Anweisungen gelten nur, wenn Sie die zentrale Konfiguration nicht verwenden.

Wählen Sie Ihre bevorzugte Zugriffsmethode und folgen Sie den Schritten, um neue Steuerungen in aktivierten Standards automatisch zu aktivieren.

 Note

Wenn Sie neue Steuerelemente mithilfe der folgenden Anweisungen automatisch aktivieren, können Sie unmittelbar nach der Veröffentlichung mit den Steuerelementen in der Konsole und programmgesteuert interagieren. Automatisch aktivierte Steuerelemente haben jedoch vorübergehend den Standardstatus Deaktiviert. Es kann mehrere Tage dauern, bis Security Hub CSPM die Kontrollfreigabe verarbeitet und die Kontrolle in Ihrem Konto als Aktiviert kennzeichnet. Während des Verarbeitungszeitraums können Sie eine Steuerung manuell aktivieren oder deaktivieren, und Security Hub CSPM behält diese Bezeichnung bei, unabhängig davon, ob Sie die automatische Steuerung aktiviert haben.

Security Hub CSPM console

Um neue Steuerungen automatisch zu aktivieren

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Einstellungen und dann die Registerkarte Allgemein aus.
3. Wählen Sie unter Steuerelemente die Option Bearbeiten aus.
4. Aktivieren Sie die Option Neue Steuerelemente in aktivierten Standards automatisch aktivieren.

5. Wählen Sie Speichern.

Security Hub CSPM API

Um neue Steuerelemente automatisch zu aktivieren

1. Führen Sie [UpdateSecurityHubConfiguration](#).
2. Um neue Steuerelemente für aktivierte Standards automatisch zu aktivieren, stellen Sie `AutoEnableControls` auf `true`. Wenn Sie neue Steuerelemente nicht automatisch aktivieren möchten, legen Sie den Wert `AutoEnableControls` auf `False` fest.

AWS CLI

Um neue Steuerelemente automatisch zu aktivieren

1. Führen Sie den Befehl [update-security-hub-configuration](#) aus.
2. Um neue Steuerelemente für aktivierte Standards automatisch zu aktivieren, geben Sie `--auto-enable-controls`. Wenn Sie neue Steuerelemente nicht automatisch aktivieren möchten, geben Sie Folgendes an `--no-auto-enable-controls`.

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

Beispielbefehl

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

Wenn Sie neue Steuerelemente nicht automatisch aktivieren, müssen Sie sie manuell aktivieren. Detaillierte Anweisungen finden Sie unter [Steuerelemente in Security Hub CSPM aktivieren](#).

Steuerelemente in Security Hub CSPM deaktivieren

Um das Suchgeräusch zu reduzieren, kann es hilfreich sein, Steuerungen zu deaktivieren, die für Ihre Umgebung nicht relevant sind. In AWS Security Hub Cloud Security Posture Management (CSPM) können Sie eine Steuerung für alle Sicherheitsstandards oder nur für bestimmte Standards deaktivieren.

Wenn Sie eine Steuerung für alle Standards deaktivieren, passiert Folgendes:

- Sicherheitsüberprüfungen für das Steuerelement werden nicht mehr durchgeführt.
- Für die Kontrolle werden keine zusätzlichen Ergebnisse generiert.
- Bestehende Ergebnisse werden für die Kontrolle nicht mehr aktualisiert.
- Bestehende Ergebnisse für die Kontrolle werden automatisch archiviert, in der Regel innerhalb von 3—5 Tagen nach bestem Wissen und Gewissen.
- Security Hub CSPM entfernt alle zugehörigen AWS Config Regeln, die es für das Steuerelement erstellt hat.

Wenn Sie ein Steuerelement nur für bestimmte Standards deaktivieren, beendet Security Hub CSPM die Ausführung von Sicherheitsüberprüfungen für das Steuerelement nur für diese Standards. Dadurch wird die Kontrolle auch aus den [Berechnungen der Sicherheitsbewertung](#) für jeden dieser Standards entfernt. Wenn die Steuerung in anderen Standards aktiviert ist, behält Security Hub CSPM die zugehörige AWS Config Regel bei, sofern zutreffend, und führt weiterhin Sicherheitsprüfungen für die Steuerung für die anderen Standards durch. Security Hub CSPM beinhaltet auch die Kontrolle bei der Berechnung der Sicherheitsbewertung für jeden der anderen Standards, was sich auf Ihre zusammenfassende Sicherheitsbewertung auswirkt.

Wenn Sie einen Standard deaktivieren, werden alle Kontrollen, die für den Standard gelten, automatisch für diesen Standard deaktiviert. Die Steuerelemente sind jedoch möglicherweise weiterhin in anderen Standards aktiviert. Wenn Sie einen Standard deaktivieren, verfolgt Security Hub CSPM nicht, welche Kontrollen für den Standard deaktiviert wurden. Wenn Sie denselben Standard zu einem späteren Zeitpunkt erneut aktivieren, werden daher alle für ihn geltenden Steuerelemente automatisch aktiviert. Hinweise zur Deaktivierung eines Standards finden Sie unter [Deaktivierung eines Standards](#)

Das Deaktivieren eines Steuerelements ist keine permanente Aktion. Angenommen, Sie deaktivieren ein Steuerelement und aktivieren dann einen Standard, der das Steuerelement enthält. Das Steuerelement wird dann für diesen Standard aktiviert. Wenn Sie einen Standard in Security Hub CSPM aktivieren, werden alle Kontrollen, die für den Standard gelten, automatisch aktiviert. Informationen zur Aktivierung eines Standards finden Sie unter [Einen Standard aktivieren](#)

Themen

- [Ein standardübergreifendes Steuerelement deaktivieren](#)
- [Deaktivierung eines Steuerelements in einem bestimmten Standard](#)

- [Vorgeschlagene Steuerelemente zur Deaktivierung in Security Hub CSPM](#)

Ein standardübergreifendes Steuerelement deaktivieren

Wir empfehlen, eine standardübergreifende AWS Security Hub Cloud Security Posture Management (CSPM) -Steuerung zu deaktivieren, um die Abstimmung in Ihrem gesamten Unternehmen aufrechtzuerhalten. Wenn Sie eine Kontrolle nur in bestimmten Standards deaktivieren, erhalten Sie weiterhin Ergebnisse für die Kontrolle, wenn sie in anderen Standards aktiviert ist.

Standardübergreifende Deaktivierung in mehreren Konten und Regionen

[Um eine Sicherheitskontrolle für mehrere AWS-Konten Länder zu deaktivieren AWS-Regionen, müssen Sie die zentrale Konfiguration verwenden.](#)

Wenn Sie die zentrale Konfiguration verwenden, kann der delegierte Administrator Security Hub CSPM-Konfigurationsrichtlinien erstellen, die bestimmte Kontrollen für alle aktivierten Standards deaktivieren. Anschließend können Sie die Konfigurationsrichtlinie bestimmten Konten oder dem Stammkonto zuordnen. OUs Eine Konfigurationsrichtlinie wird in Ihrer Heimatregion (auch Aggregationsregion genannt) und allen verknüpften Regionen wirksam.

Konfigurationsrichtlinien bieten Anpassungsmöglichkeiten. Sie können beispielsweise festlegen, dass alle AWS CloudTrail Steuerelemente in einer Organisationseinheit deaktiviert werden, und Sie können festlegen, dass alle IAM-Steuerelemente in einer anderen Organisationseinheit deaktiviert werden. Der Grad der Granularität hängt von Ihren beabsichtigten Zielen für den Sicherheitsschutz in Ihrem Unternehmen ab. Anweisungen zum Erstellen einer Konfigurationsrichtlinie, die bestimmte Kontrollen standardübergreifend deaktiviert, finden Sie unter [Konfigurationsrichtlinien erstellen und zuordnen](#)

Note

Der delegierte Administrator kann Konfigurationsrichtlinien erstellen, um Kontrollen in allen Standards außer dem [Service-Managed](#) Standard zu verwalten. AWS Control Tower Die Kontrollen für diesen Standard sollten im Service konfiguriert werden. AWS Control Tower

Wenn Sie möchten, dass einige Konten ihre eigenen Steuerungen konfigurieren und nicht der delegierte Administrator, kann der delegierte Administrator diese Konten als selbstverwaltet kennzeichnen. Selbstverwaltete Konten müssen die Kontrollen in jeder Region separat konfigurieren.

Standardübergreifende Deaktivierung in einem einzigen Konto und einer Region

Wenn Sie keine zentrale Konfiguration verwenden oder ein selbstverwaltetes Konto haben, können Sie keine Konfigurationsrichtlinien verwenden, um Steuerungen in mehreren Konten und Regionen zentral zu deaktivieren. Sie können jedoch eine Steuerung für ein einzelnes Konto und eine Region deaktivieren.

Security Hub CSPM console

Um ein standardübergreifendes Steuerelement in einem Konto und einer Region zu deaktivieren

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Controls aus.
3. Wählen Sie die Option neben einem Steuerelement aus.
4. Wählen Sie Steuerung deaktivieren. Diese Option wird nicht für ein Steuerelement angezeigt, das bereits deaktiviert ist.
5. Wählen Sie einen Grund für die Deaktivierung des Steuerelements aus und bestätigen Sie, indem Sie Deaktivieren wählen.
6. Wiederholen Sie den Vorgang in jeder Region, in der Sie das Steuerelement deaktivieren möchten.

Security Hub CSPM API

Um ein Steuerelement standardübergreifend in einem Konto und einer Region zu deaktivieren

1. Rufen Sie die [ListStandardsControlAssociations](#)API auf. Geben Sie eine Sicherheitskontroll-ID an.

Beispiel für eine Anfrage:

```
{
  "SecurityControlId": "IAM.1"
}
```

2. Rufen Sie die [BatchUpdateStandardsControlAssociations](#)API auf. Geben Sie den ARN aller Standards an, in denen das Steuerelement aktiviert ist. Führen Sie den Befehl aus ARNs, um den Standard abzurufen [DescribeStandards](#).

3. Stellen Sie den `AssociationStatus` Parameter auf `DISABLED`. Wenn Sie diese Schritte für ein Steuerelement ausführen, das bereits deaktiviert ist, gibt die API eine Antwort mit dem HTTP-Statuscode 200 zurück.

Beispiel für eine Anfrage:

```
{
  "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-
benchmark/v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not
applicable to environment"}, {"SecurityControlId": "IAM.1", "StandardsArn":
"arn:aws:securityhub::standards/aws-foundational-security-best-practices/
v/1.0.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
environment"}]]
}
```

4. Wiederholen Sie dies in jeder Region, in der Sie das Steuerelement deaktivieren möchten.

AWS CLI

Um ein Steuerelement standardübergreifend in einem Konto und einer Region zu deaktivieren

1. Führen Sie den Befehl [list-standards-control-associations](#) aus. Geben Sie eine ID für die Sicherheitskontrolle ein.

```
aws securityhub --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. Führen Sie den Befehl [batch-update-standards-control-associations](#) aus. Geben Sie den ARN aller Standards an, in denen das Steuerelement aktiviert ist. Führen Sie den `describe-standards` Befehl aus ARNs, um den Standard zu erhalten.
3. Stellen Sie den `AssociationStatus` Parameter auf `DISABLED`. Wenn Sie diese Schritte für ein Steuerelement ausführen, das bereits deaktiviert ist, gibt der Befehl eine Antwort mit dem HTTP-Statuscode 200 zurück.

```
aws securityhub --region us-east-1 batch-update-standards-control-associations
--standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
"StandardsArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable
to environment"}, {"SecurityControlId": "CloudTrail.1", "StandardsArn":
```

```
"arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/v/1.4.0",  
"AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to  
environment"}]}
```

4. Wiederholen Sie den Vorgang in jeder Region, in der Sie das Steuerelement deaktivieren möchten.

Deaktivierung eines Steuerelements in einem bestimmten Standard

Sie können ein Steuerelement nur für bestimmte Sicherheitsstandards deaktivieren, anstatt für alle Standards. Wenn die Kontrolle für andere aktivierte Standards gilt, führt AWS Security Hub Cloud Security Posture Management (CSPM) weiterhin Sicherheitsprüfungen für die Kontrolle durch und Sie erhalten weiterhin Ergebnisse für die Kontrolle.

Wir empfehlen, den Aktivierungsstatus einer Kontrolle auf alle aktivierten Standards abzustimmen, für die die Kontrolle gilt. Informationen zur Deaktivierung eines Steuerelements für alle Standards, für die es gilt, finden Sie unter [Ein standardübergreifendes Steuerelement deaktivieren](#)

Auf der Seite mit den Standarddetails können Sie auch Steuerelemente in bestimmten Standards deaktivieren. Sie müssen die Steuerelemente in bestimmten Standards in jedem AWS-Konto und separat deaktivieren AWS-Region. Wenn Sie ein Steuerelement in bestimmten Standards deaktivieren, wirkt sich dies nur auf das Girokonto und die Region aus.

Wählen Sie Ihre bevorzugte Methode und gehen Sie wie folgt vor, um ein Steuerelement in einem oder mehreren bestimmten Standards zu deaktivieren.

Security Hub CSPM console

Um ein Steuerelement in einem bestimmten Standard zu deaktivieren

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Sicherheitsstandards aus. Wählen Sie Ergebnisse anzeigen für den entsprechenden Standard aus.
3. Wählen Sie ein Steuerelement aus.
4. Wählen Sie Steuerung deaktivieren. Diese Option wird nicht für ein Steuerelement angezeigt, das bereits deaktiviert ist.

5. Geben Sie einen Grund für die Deaktivierung des Steuerelements an und bestätigen Sie, indem Sie Deaktivieren wählen.

Security Hub CSPM API

Um ein Steuerelement in einem bestimmten Standard zu deaktivieren

1. Führen Sie [ListSecurityControlDefinitions](#) einen Standard-ARN aus und geben Sie ihn an, um eine Liste der verfügbaren Steuerelemente für einen bestimmten Standard abzurufen. Führen Sie den Befehl aus, um einen Standard-ARN zu erhalten [DescribeStandards](#). Diese API gibt eine standardunabhängige Sicherheitskontrolle zurück IDs, keine standardspezifische Steuerung. IDs

Beispiel für eine Anfrage:

```
{
  "StandardsArn": "arn:aws:securityhub::standards/aws-foundational-security-
  best-practices/v/1.0.0"
}
```

2. Führen Sie [ListStandardsControlAssociations](#) den Vorgang aus und geben Sie eine spezifische Kontroll-ID an, um den aktuellen Aktivierungsstatus eines Steuerelements in jedem Standard zurückzugeben.

Beispiel für eine Anfrage:

```
{
  "SecurityControlId": "IAM.1"
}
```

3. Führen Sie [BatchUpdateStandardsControlAssociations](#). Geben Sie den ARN des Standards an, in dem Sie das Steuerelement deaktivieren möchten.
4. Stellen Sie den AssociationStatus Parameter aufDISABLED. Wenn Sie diese Schritte für ein Steuerelement ausführen, das bereits deaktiviert ist, gibt die API eine Antwort mit dem HTTP-Statuscode 200 zurück.

Beispiel für eine Anfrage:

```
{
```

```
"StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
  "StandardsArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
environment"}]
}
```

AWS CLI

Um ein Steuerelement in einem bestimmten Standard zu deaktivieren

1. Führen Sie den [list-security-control-definitions](#) Befehl aus und geben Sie einen Standard-ARN an, um eine Liste der verfügbaren Steuerelemente für einen bestimmten Standard abzurufen. Führen Sie den Befehl aus, um einen Standard-ARN zu erhalten `describe-standards`. Dieser Befehl gibt eine standardunabhängige Sicherheitskontrolle zurück IDs, keine standardspezifische Steuerung. IDs

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. Führen Sie den [list-standards-control-associations](#) Befehl aus und geben Sie eine spezifische Kontroll-ID an, um den aktuellen Aktivierungsstatus eines Steuerelements in jedem Standard zurückzugeben.

```
aws securityhub --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. Führen Sie den Befehl [batch-update-standards-control-associations](#) aus. Geben Sie den ARN des Standards an, in dem Sie das Steuerelement deaktivieren möchten.
4. Stellen Sie den `AssociationStatus` Parameter auf `DISABLED`. Wenn Sie diese Schritte für ein Steuerelement ausführen, das bereits aktiviert ist, gibt der Befehl eine Antwort mit dem HTTP-Statuscode 200 zurück.

```
aws securityhub --region us-east-1 batch-update-standards-control-
associations --standards-control-association-updates '[{"SecurityControlId":
"CloudTrail.1", "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0", "AssociationStatus": "DISABLED",
"UpdatedReason": "Not applicable to environment"}]'
```

Vorgeschlagene Steuerelemente zur Deaktivierung in Security Hub CSPM

Wir empfehlen, einige AWS Security Hub Cloud Security Posture Management (CSPM) -Kontrollen zu deaktivieren, um das Suchgeräusch und die Nutzungskosten zu reduzieren.

Kontrollen, die globale Ressourcen verwenden

Einige AWS-Services unterstützen globale Ressourcen, was bedeutet, dass Sie von jeder Ressource aus auf die Ressource zugreifen können AWS-Region. Um Kosten zu sparen AWS Config, können Sie die Aufzeichnung globaler Ressourcen in allen Regionen außer einer Region deaktivieren. Nachdem Sie dies getan haben, führt Security Hub CSPM jedoch weiterhin Sicherheitsüberprüfungen in allen Regionen durch, in denen eine Kontrolle aktiviert ist, und berechnet Ihnen Gebühren auf der Grundlage der Anzahl der Prüfungen pro Konto pro Region. Um das Suchrauschen zu reduzieren und die Kosten für Security Hub CSPM zu senken, sollten Sie daher auch Kontrollen deaktivieren, die globale Ressourcen in allen Regionen betreffen, mit Ausnahme der Region, in der globale Ressourcen erfasst werden.

Wenn ein Steuerelement globale Ressourcen umfasst, aber nur in einer Region verfügbar ist, können Sie, wenn Sie es in dieser Region deaktivieren, keine Ergebnisse für die zugrunde liegende Ressource abrufen. In diesem Fall empfehlen wir, das Steuerelement aktiviert zu lassen. Wenn Sie die regionsübergreifende Aggregation verwenden, sollte die Region, in der das Steuerelement verfügbar ist, die Aggregationsregion oder eine der verknüpften Regionen sein. Die folgenden Steuerelemente beziehen sich auf globale Ressourcen, sind jedoch nur in einer einzigen Region verfügbar:

- Alle CloudFront Steuerelemente — Nur in der Region USA Ost (Nord-Virginia) verfügbar
- GlobalAccelerator.1 — Nur in der Region USA West (Oregon) verfügbar
- Route 53.2 — Nur in der Region USA Ost (Nord-Virginia) verfügbar
- WAF.1, WAF.6, WAF.7, WAF.8 — Nur in der Region USA Ost (Nord-Virginia) verfügbar

Note

Wenn Sie die zentrale Konfiguration verwenden, deaktiviert Security Hub CSPM automatisch Kontrollen, die globale Ressourcen in allen Regionen außer der Heimatregion betreffen. Andere Steuerelemente, die Sie über eine Konfigurationsrichtlinie aktivieren, sind in allen Regionen aktiviert, in denen sie verfügbar sind. Um die Ergebnisse für diese Steuerelemente auf nur eine Region zu beschränken, können Sie Ihre AWS Config Rekordereinstellungen

aktualisieren und die globale Ressourcenaufzeichnung in allen Regionen außer der Heimatregion deaktivieren.

Wenn ein aktiviertes Steuerelement, das globale Ressourcen umfasst, in der Heimatregion nicht unterstützt wird, versucht Security Hub CSPM, das Steuerelement in einer verknüpften Region zu aktivieren, in der das Steuerelement unterstützt wird. Bei zentraler Konfiguration fehlt Ihnen die Abdeckung für ein Steuerelement, das in der Heimatregion oder einer der verknüpften Regionen nicht verfügbar ist.

Weitere Informationen zur zentralen Konfiguration finden Sie unter [Grundlegendes zur zentralen Konfiguration in Security Hub CSPM](#).

Für Kontrollen mit einem periodischen Zeitplantyp ist es erforderlich, sie in Security Hub CSPM zu deaktivieren, um eine Abrechnung zu verhindern. Die Einstellung des AWS Config Parameters `includeGlobalResourceTypes` auf `false` hat keinen Einfluss auf regelmäßige Security Hub CSPM-Steuerungen.

Die folgenden Security Hub CSPM-Steuerelemente verwenden globale Ressourcen:

- [\[Account.1\] Sicherheitskontaktinformationen sollten bereitgestellt werden für AWS-Konto](#)
- [\[Account.2\] AWS-Konten sollte Teil einer Organisation sein AWS Organizations](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)

- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[IAM.1\] IAM-Richtlinien sollten keine vollen „*“-Administratorrechte zulassen](#)
- [\[IAM.2\] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein](#)
- [\[IAM.3\] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden](#)
- [\[IAM.4\] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren](#)
- [\[IAM.5\] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen](#)
- [\[IAM.6\] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.](#)
- [\[IAM.7\] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein](#)
- [\[IAM.8\] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden](#)
- [\[IAM.9\] MFA sollte für den Root-Benutzer aktiviert sein](#)
- [\[IAM.10\] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein](#)
- [\[IAM.11\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert](#)
- [\[IAM.12\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert](#)
- [\[IAM.13\] Stellen Sie sicher, dass für die IAM-Passwortrichtlinie mindestens ein Symbol erforderlich ist](#)
- [\[IAM.14\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert](#)
- [\[IAM.15\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert](#)
- [\[IAM.16\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert](#)
- [\[IAM.17\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft](#)
- [\[IAM.18\] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS -Support](#)
- [\[IAM.19\] MFA sollte für alle IAM-Benutzer aktiviert sein](#)

- [\[IAM.21\] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen](#)
- [\[IAM.22\] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden](#)
- [\[IAM.24\] IAM-Rollen sollten mit Tags versehen werden](#)
- [\[IAM.25\] IAM-Benutzer sollten markiert werden](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[IAM.27\] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWS Cloud Shell FullAccess](#)
- [\[KMS.1\] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)
- [\[KMS.2\] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)

CloudTrail Steuerelemente zur Protokollierung

Dieses Steuerelement befasst sich mit der Verwendung von AWS Key Management Service (AWS KMS) zur Verschlüsselung von AWS CloudTrail Trail-Logs. Wenn Sie diese Pfade in einem zentralen Protokollierungskonto protokollieren, müssen Sie diese Steuerung nur in dem Konto und der Region aktivieren, in der die zentrale Protokollierung stattfindet.

Note

Wenn Sie die [zentrale Konfiguration](#) verwenden, wird der Aktivierungsstatus eines Steuerelements auf die Heimatregion und die verknüpften Regionen verteilt. Sie können ein Steuerelement nicht in einigen Regionen deaktivieren und in anderen aktivieren. Unterdrücken Sie in diesem Fall die Ergebnisse der folgenden Steuerelemente, um das Suchrauschen zu reduzieren.

- [\[CloudTrail.2\] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben](#)

CloudWatch Alarmsteuerungen

Wenn Sie Amazon GuardDuty für die Erkennung von Anomalien anstelle von CloudWatch Amazon-Alarmen bevorzugen, können Sie die folgenden Steuerungen deaktivieren, die sich auf CloudWatch Alarme konzentrieren:

- [\[CloudWatch.1\] Für den Benutzer „root“ sollten ein Filter und ein Alarm für die Log-Metrik vorhanden sein](#)
- [\[CloudWatch.2\] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für nicht autorisierte API-Aufrufe vorhanden sind](#)
- [\[CloudWatch.3\] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für die Anmeldung in der Managementkonsole ohne MFA vorhanden sind](#)
- [\[CloudWatch.4\] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der IAM-Richtlinie vorhanden sind](#)
- [\[CloudWatch.5\] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für CloudTrail -Config--Config-Änderungen vorhanden sind](#)
- [\[CloudWatch.6\] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für AWS Management Console Authentifizierungsfehler vorhanden sind](#)
- [\[CloudWatch.7\] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden verwalteten Schlüsseln vorhanden sind](#)
- [\[CloudWatch.8\] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der S3-Bucket-Richtlinie vorhanden sind](#)
- [\[CloudWatch.9\] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für AWS Config -Config--Config-Änderungen vorhanden sind](#)
- [\[CloudWatch.10\] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Sicherheitsgruppe vorhanden sind](#)
- [\[CloudWatch.11\] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an den Network Access Control Lists \(NACL\) vorhanden sind](#)
- [\[CloudWatch.12\] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an Network-Gateways vorhanden sind](#)
- [\[CloudWatch.13\] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Routing-Tabelle vorhanden sind](#)

- [\[CloudWatch.14\] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für VPC-Änderungen vorhanden sind](#)

Grundlegendes zu Sicherheitsüberprüfungen und Bewertungen in Security Hub CSPM

Für jedes Steuerelement, das Sie aktivieren, führt AWS Security Hub Cloud Security Posture Management (CSPM) Sicherheitsprüfungen durch. Eine Sicherheitsüberprüfung führt zu einem Ergebnis, das Ihnen Aufschluss darüber gibt, ob eine bestimmte AWS Ressource den in der Kontrolle enthaltenen Regeln entspricht.

Einige Prüfungen werden in regelmäßigen Abständen ausgeführt. Andere Prüfungen werden nur ausgeführt, wenn sich der Ressourcenstatus ändert. Weitere Informationen finden Sie unter [Zeitplan für die Ausführung von Sicherheitsprüfungen](#).

Viele Sicherheitsüberprüfungen verwenden AWS Config verwaltete oder benutzerdefinierte Regeln, um die Konformitätsanforderungen festzulegen. Um diese Prüfungen durchzuführen, müssen Sie die Ressourcenaufzeichnung für die erforderlichen Ressourcen einrichten AWS Config und aktivieren. Weitere Informationen zur Einrichtung finden Sie AWS Config unter [Aktivierung und Konfiguration AWS Config für Security Hub CSPM](#). Eine Liste der AWS Config Ressourcen, die Sie für jeden Standard aufzeichnen müssen, finden Sie unter [Erforderliche AWS Config Ressourcen für Kontrollbefunde](#). Andere Steuerelemente verwenden benutzerdefinierte Lambda-Funktionen, die von Security Hub CSPM verwaltet werden und keine Voraussetzungen erfordern.

Während Security Hub CSPM Sicherheitsüberprüfungen durchführt, generiert es Ergebnisse und weist ihnen einen Compliance-Status zu. Weitere Informationen zum Compliance-Status finden Sie unter [Bewertung des Compliance-Status der CSPM-Ergebnisse von Security Hub](#).

Security Hub CSPM verwendet den Compliance-Status von Kontrollfeststellungen, um einen allgemeinen Kontrollstatus zu ermitteln. Auf der Grundlage des Kontrollstatus berechnet Security Hub CSPM außerdem eine Sicherheitsbewertung für alle aktivierten Kontrollen und für bestimmte Standards. Weitere Informationen erhalten Sie unter [the section called “Konformitätsstatus und Kontrollstatus”](#) und [the section called “Berechnung von Sicherheitswerten”](#).

Wenn Sie konsolidierte Kontrollergebnisse aktiviert haben, generiert Security Hub CSPM auch dann ein einziges Ergebnis, wenn eine Kontrolle mit mehr als einem Standard verknüpft ist. Weitere Informationen finden Sie unter [Konsolidierte Kontrollergebnisse](#).

Themen

- [Erforderliche AWS Config Ressourcen für Kontrollbefunde](#)
- [Zeitplan für die Ausführung von Sicherheitsprüfungen](#)
- [Generierung und Aktualisierung von Kontrollbefunden](#)
- [Bewertung des Konformitätsstatus und des Kontrollstatus](#)
- [Berechnung von Sicherheitswerten](#)

Erforderliche AWS Config Ressourcen für Kontrollbefunde

In AWS Security Hub Cloud Security Posture Management (CSPM) verwenden einige Kontrollen dienstbezogene AWS Config Regeln, die Konfigurationsänderungen in Ihren Ressourcen erkennen. AWS Damit Security Hub CSPM genaue Ergebnisse für diese Kontrollen generiert, müssen Sie die Ressourcenaufzeichnung in aktivieren AWS Config und einschalten. AWS Config Informationen darüber, wie Security Hub CSPM AWS Config Regeln verwendet und wie sie aktiviert und konfiguriert werden AWS Config, finden Sie unter. [Aktivierung und Konfiguration AWS Config für Security Hub CSPM](#) Ausführliche Informationen zur Ressourcenaufzeichnung finden Sie unter [Arbeiten mit dem Konfigurationsrekorder](#) im AWS Config Entwicklerhandbuch.

Um genaue Kontrollergebnisse zu erhalten, müssen Sie die AWS Config Ressourcenaufzeichnung für aktivierte Steuerelemente mit einem durch Änderung ausgelösten Zeitplantyp aktivieren. Für einige Steuerelemente mit einem periodischen Zeitplan ist auch eine Ressourcenaufzeichnung erforderlich. Auf dieser Seite sind die erforderlichen Ressourcen für diese Security Hub CSPM-Steuerelemente aufgeführt.

Security Hub CSPM-Steuerungen können auf verwalteten AWS Config Regeln oder benutzerdefinierten Security Hub CSPM-Regeln basieren. Stellen Sie sicher, dass es keine AWS Identity and Access Management (IAM-) Richtlinien oder AWS Organizations verwalteten Richtlinien gibt, die AWS Config verhindern, dass Sie Ihre Ressourcen aufzeichnen dürfen. Die CSPM-Steuerungen von Security Hub werten Ressourcenkonfigurationen direkt aus und berücksichtigen keine AWS Organizations Richtlinien.

Note

AWS-Regionen Wenn ein Steuerelement nicht verfügbar ist, ist die entsprechende Ressource in nicht verfügbar. AWS Config Eine Liste dieser Grenzwerte finden Sie unter [Regionale Beschränkungen der Security Hub CSPM-Steuerungen](#).

Themen

- [Erforderliche Ressourcen für alle Security Hub CSPM-Steuerelemente](#)
- [Erforderliche Ressourcen für den Standard „Best Practices für AWS grundlegende Sicherheit“](#)
- [Erforderliche Ressourcen für den CIS AWS Foundations Benchmark](#)
- [Erforderliche Ressourcen für den Standard NIST SP 800-53 Revision 5](#)
- [Erforderliche Ressourcen für den Standard NIST SP 800-171 Revision 2](#)
- [Erforderliche Ressourcen für PCI DSS v3.2.1](#)
- [Erforderliche Ressourcen für den AWS Resource Tagging-Standard](#)
- [Erforderliche Ressourcen für den AWS Control Tower Service-Managed-Standard](#)

Erforderliche Ressourcen für alle Security Hub CSPM-Steuerelemente

Damit Security Hub CSPM Ergebnisse für durch Änderungen ausgelöste Kontrollen generiert, die aktiviert sind und eine AWS Config Regel verwenden, müssen Sie die folgenden Ressourcentypen in aufzeichnen. AWS Config In dieser Tabelle ist auch angegeben, mit welchen Kontrollen ein bestimmter Ressourcentyp bewertet wird. Ein einzelnes Steuerelement kann mehr als einen Ressourcentyp auswerten.

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
AWS Amplify	AWS::Amplify::App	Verstärker.1
	AWS::Amplify::Branch	Verstärker.2
Amazon API Gateway	AWS::ApiGateway::Stage	APIGateway1.
		APIGateway2.
		APIGateway3.
		APIGateway4.
		APIGateway5.

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
AWS AppConfig	AWS::ApiGatewayV2::Stage	APIGateway1. APIGateway9.
	AWS::AppConfig::Application	AppConfig1.
	AWS::AppConfig::ConfigurationProfile	AppConfig2.
	AWS::AppConfig::Environment	AppConfig3.
	AWS::AppConfig::ExtensionAssociation	AppConfig4.
Amazon AppFlow	AWS::AppFlow::Flow	AppFlow1.
AWS App Runner	AWS::AppRunner::Service	AppRunner1.
	AWS::AppRunner::VpcConnector	AppRunner2.
AWS AppSync	AWS::AppSync::GraphQLApi	AppSync2. AppSync4. AppSync5.

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	AWS::AppSync::ApiCache	AppSync1. AppSync6.
AWS Backup	AWS::Backup::BackupPlan	Sicherung.5
	AWS::Backup::BackupVault	Sicherung.3
	AWS::Backup::RecoveryPoint	Sicherung.1 Sicherung.2
	AWS::Backup::ReportPlan	Sicherung.4
AWS Batch	AWS::Batch::ComputeEnvironment	Charge.3 Charge.4
	AWS::Batch::JobQueue	Charge.1
	AWS::Batch::SchedulingPolicy	Charge.2
AWS Certificate Manager (ACM)	AWS::ACM::Certificate	ACM.1 ACM.2 ACM. 3
Amazon Athena	AWS::Athena::DataCatalog	Athena.2

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	AWS::Athena::WorkGroup	Athena.3 Athena.4
AWS CloudFormation	AWS::CloudFormation::Stack	CloudFormation2.
Amazon CloudFront	AWS::CloudFront::Distribution	CloudFront1. CloudFront3. CloudFront4. CloudFront5. CloudFront6. CloudFront.7 CloudFront.8 CloudFront.9 CloudFront.10 CloudFront.13 CloudFront.14 CloudFront.15
AWS CloudTrail	AWS::CloudTrail::Trail	CloudTrail.9
Amazon CloudWatch	AWS::CloudWatch::Alarm	CloudWatch1,5 CloudWatch.17

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
AWS CodeArtifact	AWS::CodeArtifact::Repository	CodeArtifact1.
AWS CodeBuild	AWS::CodeBuild::Project	CodeBuild1. CodeBuild2. CodeBuild3. CodeBuild4.
	AWS::CodeBuild::ReportGroup	CodeBuild.7
CodeGuru Amazon-Profiler	AWS::CodeGuruProfiler::ProfilingGroup	CodeGuruProfiler1.
CodeGuru Amazon-Rezensent	AWS::CodeGuruReviewer::RepositoryAssociation	CodeGuruReviewer1.
Amazon Cognito	AWS::Cognito::IdentityPool	Kognito. 2
	AWS::Cognito::UserPool	Kognito. 1

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
Amazon Connect	AWS::CustomerProfiles::ObjectType	Verbinden.1
	AWS::Connect::Instance	Verbinden.2
AWS DataSync	AWS::DataSync::Task	DataSync1. DataSync2.
Amazon Detective	AWS::Detective::Graph	Detektiv.1
AWS Database Migration Service (AWS DMS)	AWS::DMS::Certificate	DMS.2
	AWS::DMS::Endpoint	DMS. 9
		DMS.10
		DMS.11
		DMS.12
	AWS::DMS::EventSubscription	DMS.3
	AWS::DMS::ReplicationInstance	DMS.4
		DMS.6
	AWS::DMS::ReplicationSubnetGroup	DMS. 5

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
Amazon-DynamoDB	AWS::DMS: :ReplicationTask	DMS. 7 DMS. 8
	AWS::DynamoDB::Table	DynamoDB.1 DynamoDB.2 Dynamo DB.5 Dynamo DB,6
	AWS::EC2: :ClientVpnEndpoint	EC25.1
	AWS::EC2: :CustomerGateway	EC23,6
	AWS::EC2: :DHCPOptions	EC2.174
	AWS::EC2::EIP	EC2.12 EC2.37
	AWS::EC2: :FlowLog	EC24,8

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	AWS::EC2: :Instance	EC24. EC2.8 EC2.9 EC2.17 EC2.24 EC23,8 EMR.1 SSM.1
	AWS::EC2: :Internet Gateway	EC2.39
	AWS::EC2: :LaunchTe mplate	EC2.25 EC21,70 EC21,75
	AWS::EC2: :NatGateway	EC2.40
	AWS::EC2: :NetworkAc1	EC2.16 EC2.21 EC24,1
	AWS::EC2: :NetworkI nterface	EC2.22 EC2.35 EC21,80

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	AWS::EC2: :PrefixList	EC2.176
	AWS::EC2: :RouteTable	EC24,2
	AWS::EC2: :SecurityGroup	EC22.
		EC2.13
		EC2.14
		EC2.18
		EC2.19
		EC24,3
	AWS::EC2: :SpotFleet	EC2.173
	AWS::EC2: :Subnet	EC2,15
		EC24,4
		ElastiCache.7
	AWS::EC2: :TrafficMirrorFilter	EC2.178
	AWS::EC2: :TrafficMirrorSession	EC2.177
	AWS::EC2: :TrafficMirrorTarget	EC2,179

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	AWS::EC2: :TransitGateway	EC2.23 EC25,2
	AWS::EC2: :TransitGatewayAttachment	EC2.33
	AWS::EC2: :TransitGatewayRouteTable	EC2.34
	AWS::EC2: :Volume	EC23. EC24,5
	AWS::EC2::VPC	EC2.6 EC24,6
	AWS::EC2: :VPCBlockPublicAccessOptions	EC21,72
	AWS::EC2: :VPCEndpointService	EC24,7
	AWS::EC2: :VPCPeeringConnection	EC24,9

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	AWS::EC2: :VPNConnection	EC2.20 EC2.171
	AWS::EC2: :VPNGateway	EC25,0
Amazon EC2 Auto Scaling	AWS::AutoScaling::AutoScalingGroup	AutoScaling1. AutoScaling2. AutoScaling6. AutoScaling.9 AutoScaling.10
	AWS::AutoScaling::LaunchConfiguration	AutoScaling3. AutoScaling.5
EC2 Amazon-Systemmanager (SSM)	AWS::SSM::AssociationCompliance	SSM.3
	AWS::SSM::ManagedInstanceInventory	SSM.1
	AWS::SSM::PatchCompliance	SSM.2
Amazon Elastic Container Registry (Amazon ECR)	AWS::ECR::PublicRepository	ECR. 4

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	AWS::ECR: :Repository	ECR.2 ECR.3 EKR.5
Amazon Elastic Container Service (Amazon ECS)	AWS::ECS: :Cluster	ECS.12 SEK. 14
	AWS::ECS: :Service	ECS.2 ECS.10 SEK. 13
	AWS::ECS: :TaskDefinition	ECS.1 ECS.3 ECS.4 ECS.5 ECS.8 SEK. 9 SEK. 15 SEK. 17
	AWS::ECS: :TaskSet	SEK. 16
Amazon Elastic File System (Amazon EFS)	AWS::EFS: :AccessPoint	EFS.3 EFS.4 EFS. 5

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	AWS::EFS: :FileSystem	EFS 7 EFS. 8
Amazon Elastic Kubernetes Service (Amazon EKS)	AWS::EKS: :Cluster	EKS.2 EKS.6 EKS.8
	AWS::EKS: :Identity ProviderConfig	EKS.7
AWS Elastic Beanstalk	AWS::ElasticBeanstalk::Environment	ElasticBeanstalk1. ElasticBeanstalk2. ElasticBeanstalk3.
Elastic Load Balancing	AWS::ElasticLoadBalancing:: LoadBalancer	ELB.2 ELB.3 ELB.5 ELB.7 ELB.8 ELB.9 ELB.10 ELB.14
	AWS::ElasticLoadBalancingV2:: Listener	ELB. 17 ELB. 18

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	AWS::ElasticLoadBalancingV2::LoadBalancer	ELB.1
		ELB.4
		ELB.5
		ELB.6
		ELB.12
		ELB.13
		ELB. 16
ElasticSearch	AWS::Elasticsearch::Domain	ES.3
		ES.4
		ES.5
		ES.6
		ES.7
		ES.8
		ES.9
Amazon EMR	AWS::EMR::SecurityConfiguration	EMR. 3
		EMR. 4
Amazon EventBridge	AWS::Events::EventBus	EventBridge2. EventBridge3.
	AWS::Events::Endpoint	EventBridge4.

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
Amazon Fraud Detector	AWS::FraudDetector::EntityType	FraudDetector1.
	AWS::FraudDetector::Label	FraudDetector2.
	AWS::FraudDetector::Outcome	FraudDetector3.
	AWS::FraudDetector::Variable	FraudDetector4.
AWS Global Accelerator	AWS::GlobalAccelerator::Accelerator	GlobalAccelerator1.
AWS Glue	AWS::Glue::Job	Kleber.1 Kleber.4
	AWS::Glue::MLTransform	Kleber.3
Amazon GuardDuty	AWS::GuardDuty::Detector	GuardDuty4.
	AWS::GuardDuty::Filter	GuardDuty2.
	AWS::GuardDuty::IPSet	GuardDuty3.

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
AWS Identity and Access Management (ICH BIN)	AWS::IAM::Group	ICH BIN 0,27 KMS.2
	AWS::IAM::Policy	IAM.1 IAM.21 KMS.1
	AWS::IAM::Role	ICH BIN 24 ICH BIN. 27 KMS.2
	AWS::IAM::User	IAM.2 IAM.3 IAM.5 IAM.8 ICH BIN. 19 IAM.22 ICH BIN 25 ICH BIN 27 KMS.2
AWS Identity and Access Management Access Analyzer	AWS::AccessAnalyzer::Analyzer	ICH BIN 23

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
Amazon Interacti ve Video Service (Amazon IVS)	AWS::IVS: :Playback KeyPair	IVS.1
	AWS::IVS: :Recordin gConfiguration	IVS.2
	AWS::IVS: :Channel	IVS.3
AWS IoT	AWS::IoT: :Authorizer	IoT.4
	AWS::IoT: :Dimension	IoT.3
	AWS::IoT: :Mitigati onAction	IoT.2
	AWS::IoT: :Policy	IoT. 6
	AWS::IoT: :RoleAlias	IoT.5
	AWS::IoT: :Security Profile	IoT. 1
AWS IoT Events	AWS::IoTE vents::Al armModel	IoT TEvents 3.

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	AWS::IoTEvents::DetectorModel	IoTEvents 3,2
	AWS::IoTEvents::Input	IoTEvents 1.
AWS IoT SiteWise	AWS::IoTSiteWise::AssetModel	IoTSiteWise. 1
	AWS::IoTSiteWise::Dashboard	IoTSiteWise.2 TSite
	AWS::IoTSiteWise::Gateway	IoTSiteWise.3 TSite
	AWS::IoTSiteWise::Portal	IoTSiteWise.4 TSite
	AWS::IoTSiteWise::Project	IoTSiteWise.5 TSite
AWS IoT TwinMaker	AWS::IoTThingMaker::Entity	IoTThingMaker.4
	AWS::IoTThingMaker::Scene	IoTThingMaker.3 TTwin

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	AWS::IoTwinMaker:SyncJob	Ich bin Maker.1 TTwin
	AWS::IoTwinMaker:Workspace	Ich bin Maker.2 TTwin
AWS IoT Wireless	AWS::IoTWireless::MulticastGroup	IoT TWireless 1.
	AWS::IoTWireless::ServiceProfile	IoT TWireless 1.2
	AWS::IoTWireless::FirmwareTask	IoT TWireless 3.
Amazon Keyspaces (für Apache Cassandra)	AWS::Cassandra::Keyspace	Tastenfelder.1
Amazon Kinesis	AWS::Kinesis::Stream	Kinesis.1 Kinesis.2 Kinesis.3
AWS Key Management Service (AWS KMS)	AWS::KMS::Alias	S3.17
	AWS::KMS::Key	KMS.3 KM. 5 S 3,17

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
AWS Lambda	AWS::Lambda::Function	Lambda.1
		Lambda.2
		Lambda.3
		Lambda.5
		Lambda.6
		Lambda.7
Amazon MSK	AWS::MSK::Cluster	MASKE. 1
		MSK.2
		MSK.4
		MSK.6
	AWS::KafkaConnect::Connector	MSK.3 MSK.5
Amazon MQ	AWS::AmazonMQ::Broker	MQ. 2
		MQ. 3
		MQ. 4
		MQ.5
		MQ.6

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
AWS Network Firewall	AWS::NetworkFirewall::Firewall	NetworkFirewall1. NetworkFirewall7. NetworkFirewall.9 NetworkFirewall.10
	AWS::NetworkFirewall::FirewallPolicy	NetworkFirewall3. NetworkFirewall4. NetworkFirewall5. NetworkFirewall.8
	AWS::NetworkFirewall::RuleGroup	NetworkFirewall.6

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
OpenSearch Amazon-Dienst	AWS::OpenSearch::Domain	OpenSearch.1 OpenSearch.2 OpenSearch.3 OpenSearch.4 OpenSearch.5 OpenSearch.6 OpenSearch.7 OpenSearch.8 Suche öffnen.9 Öffne Suche.10 Öffne Suche.11
AWS Private CA	AWS::ACMPCA::CertificateAuthority	STK.2

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBCluster	DocumentDB DB.1 DocumentDB DB.2 DocumentDB DB.4 DocumentDB DB.5 Neptun.1 Neptun.2 Neptun.4 Neptun.5 Neptun.7 Neptun.8 Neptun.9 RDS.7 RDS.12 RDS.14 RDS.15 RDS.16 RDS.24 RDS. 27 RDS. 28 RDS. 34 RDS.35

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
		RDS. 37
	AWS::RDS:	DocumentDB DB.3
	:DBClusterSnapshot	Neptun.3
		Neptun.6
		RDS.1
		RDS.4
		RDS. 29

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	AWS::RDS: DBInstance	RDS.2
		RDS.3
		RDS.5
		RDS.6
		RDS.8
		RDS.9
		RDS.10
		RDS.11
		RDS.13
		RDS.17
		RDS.18
		RDS.23
		RDS.25
		RDS.30
		RDS. 36
		RDS. 40
	AWS::RDS: DBSecurityGroup	RDS. 31

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	AWS::RDS: :DBSnapshot	RDS.1 RDS.4 RDS.32
	AWS::RDS: :DBSubnetGroup	RDS.33
	AWS::RDS: :EventSubscription	RDS.19 RDS.20 RDS.21 RDS.22
Amazon Redshift	AWS::Redshift::Cluster	Redshift.1 Redshift.2 Redshift.3 Redshift.4 Redshift.6 Redshift.7 Redshift.8 Redshift.9 Redshift.10 Rotverschiebung.11 Rotverschiebung.18

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	AWS::Redshift::ClusterParameterGroup	Redshift.2 Rotverschiebung.17
	AWS::Redshift::ClusterSnapshot	Rotverschiebung.13
	AWS::Redshift::ClusterSubnetGroup	Rotverschiebung.14 Rotverschiebung.16
	AWS::Redshift::EventSubscription	Rotverschiebung.12
Amazon Route 53	AWS::Route53::HostedZone	Route 53.2
	AWS::Route53::HealthCheck	Route 53.1
Amazon Simple Storage Service (Amazon-S3)	AWS::S3::AccessPoint	S3.19
	AWS::S3::AccountPublicAccessBlock	S3.2 S3.3

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	AWS::S3::Bucket	CloudTrail6. CloudTrail.7 S3.2 S3.3 S3.5 S3.6 3,7 S3.8 S3.9 S3.10 S3.11 S3.12 S3.13 S3.14 S3,15 S3,17 S3,20
	AWS::S3::MultiRegionAccessPoint	S3,24

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	AWS::S3Express::DirectoryBucket	S3,25
Amazon SageMaker KI	AWS::SageMaker::AppImageConfig	SageMaker6.
	AWS::SageMaker::Image	SageMaker.7
	AWS::SageMaker::Model	SageMaker5.
	AWS::SageMaker::NotebookInstance	SageMaker2. SageMaker3.
AWS Secrets Manager	AWS::SecretsManager::Secret	SecretsManager1. SecretsManager2. SecretsManager5.
AWS Service Catalog	AWS::ServiceCatalog::Portfolio	ServiceCatalog1.
Amazon Simple Email Service (Amazon SES)	AWS::SES::ConfigurationSet	2 SÄTZE.2
	AWS::SES::ContactList	SESS.1

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
Amazon-Simple-Notification-Service (Amazon-SNS)	AWS::SNS::Topic	SNS.1 SNS.3 SNS.4
Amazon-Simple-Queue-Service (Amazon SQS)	AWS::SQS::Queue	SQS.1 SQS.2 QUADRAT 3
AWS Step Functions	AWS::Step Functions::StateMachine	StepFunctions1.
	AWS::Step Functions::Activity	StepFunctions2.
AWS Systems Manager (SSM)	AWS::SSM::Document	SSM. 5
AWS Transfer Family	AWS::Transfer::Agreement	Übertragung.4
	AWS::Transfer::Certificate	Übertragung.5
	AWS::Transfer::Connector	Übertragung.3 Übertragung.6
	AWS::Transfer::Profile	Übertragung.7

AWS-Service	Ressourcentypen	Verwandte Steuerelemente
	AWS::Transfer::Workflow	Übertragung.1
AWS WAF	AWS::WAF::Rule	WAF.6
	AWS::WAF::RuleGroup	WAF.7
	AWS::WAF::WebACL	WAF.1 WAF.8
	AWS::WAFRegional::Rule	WAF.2
	AWS::WAFRegional::RuleGroup	WAF.3
	AWS::WAFRegional::WebACL	WAF.4
	AWS::WAFv2::RuleGroup	WAF.12
	AWS::WAFv2::WebACL	WAF.10 WAF.11
Amazon WorkSpaces	AWS::WorkSpaces::Workspace	WorkSpaces1. WorkSpaces2.

Erforderliche Ressourcen für den Standard „Best Practices für AWS grundlegende Sicherheit“

Damit Security Hub CSPM die Ergebnisse für durch Änderungen ausgelöste Kontrollen, die den Standard „Best Practices von AWS Foundation Security“ (v.1.0.0) erfüllen, aktiviert sind und eine AWS Config Regel verwenden, korrekt melden kann, müssen Sie die folgenden Ressourcentypen in aufzeichnen. AWS Config Informationen zu diesem Standard finden Sie unter [AWS Standard für grundlegende Best Practices im Bereich Sicherheit im Security Hub CSPM](#)

AWS-Service	Ressourcentypen
Amazon API Gateway	<code>AWS::ApiGateway::Stage</code> , <code>AWS::ApiGatewayV2::Stage</code>
AWS AppSync	<code>AWS::AppSync::ApiCache</code> , <code>AWS::AppSync::GraphQLApi</code>
AWS Backup	<code>AWS::Backup::RecoveryPoint</code>
AWS Certificate Manager (ACM)	<code>AWS::ACM::Certificate</code>
AWS CloudFormation	<code>AWS::CloudFormation::Stack</code>
Amazon CloudFront	<code>AWS::CloudFront::Distribution</code>
AWS CodeBuild	<code>AWS::CodeBuild::Project</code> , <code>AWS::CodeBuild::ReportGroup</code>
Amazon Cognito	<code>AWS::Cognito::IdentityPool</code> , <code>AWS::Cognito::UserPool</code>
Amazon Connect	<code>AWS::Connect::Instance</code>
AWS DataSync	<code>AWS::DataSync::Task</code>
AWS Database Migration Service (AWS DMS)	<code>AWS::DMS::Endpoint</code> , <code>AWS::DMS::ReplicationInstance</code> , <code>AWS::DMS::ReplicationTask</code>
Amazon-DynamoDB	<code>AWS::DynamoDB::Table</code>

AWS-Service	Ressourcentypen
EC2 Amazon-Systemmanager (SSM)	AWS::SSM::AssociationCompliance , AWS::SSM::ManagedInstanceInventory , AWS::SSM::PatchCompliance
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::ClientVpnEndpoint , AWS::EC2::Instance , AWS::EC2::LaunchTemplate , AWS::EC2::NetworkAcl , AWS::EC2::NetworkInterface , AWS::EC2::SecurityGroup , AWS::EC2::SpotFleet , AWS::EC2::Subnet , AWS::EC2::TransitGateway , AWS::EC2::VPCElasticNetworkConfiguration , AWS::EC2::VPNConnection , AWS::EC2::Volume
Amazon EC2 Auto Scaling	AWS::AutoScaling::AutoScalingGroup , AWS::AutoScaling::LaunchConfiguration
Amazon Elastic Container Registry (Amazon ECR)	AWS::ECR::Repository
Amazon Elastic Container Service (Amazon ECS)	AWS::ECS::Cluster , AWS::ECS::Service , AWS::ECS::TaskDefinition , AWS::ECS::TaskSet
Amazon Elastic File System (Amazon EFS)	AWS::EFS::AccessPoint , AWS::EFS::FileSystem
Amazon Elastic Kubernetes Service (Amazon EKS)	AWS::EKS::Cluster
AWS Elastic Beanstalk	AWS::ElasticBeanstalk::Environment

AWS-Service	Ressourcentypen
Elastic Load Balancing	<code>AWS::ElasticLoadBalancing::LoadBalancer</code> , <code>AWS::ElasticLoadBalancingV2::Listener</code> , <code>AWS::ElasticLoadBalancingV2::LoadBalancer</code>
ElasticSearch	<code>AWS::Elasticsearch::Domain</code>
Amazon EMR	<code>AWS::EMR::SecurityConfiguration</code>
AWS Glue	<code>AWS::Glue::Job</code> , <code>AWS::Glue::MLTransform</code>
AWS Identity and Access Management (IAM)	<code>AWS::IAM::Group</code> , <code>AWS::IAM::Policy</code> , <code>AWS::IAM::Role</code> , <code>AWS::IAM::User</code>
Amazon Kinesis	<code>AWS::Kinesis::Stream</code>
AWS Key Management Service (AWS KMS)	<code>AWS::KMS::Key</code>
AWS Lambda	<code>AWS::Lambda::Function</code>
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	<code>AWS::MSK::Cluster</code> , <code>AWS::KafkaConnect::Connector</code>
AWS Network Firewall	<code>AWS::NetworkFirewall::Firewall</code> , <code>AWS::NetworkFirewall::FirewallPolicy</code> , <code>AWS::NetworkFirewall::RuleGroup</code>
OpenSearch Amazon-Dienst	<code>AWS::OpenSearch::Domain</code>
Amazon Relational Database Service (Amazon RDS)	<code>AWS::RDS::DBCluster</code> , <code>AWS::RDS::DBClusterSnapshot</code> , <code>AWS::RDS::DBInstance</code> , <code>AWS::RDS::DBProxy</code> , <code>AWS::RDS::DBSnapshot</code> , <code>AWS::RDS::EventSubscription</code>

AWS-Service	Ressourcentypen
Amazon Redshift	<code>AWS::Redshift::Cluster</code> , <code>AWS::Redshift::ClusterSubnetGroup</code>
Amazon Redshift Serverless	<code>AWS::RedshiftServerless::Workgroup</code>
Amazon Route 53	<code>AWS::Route53::HostedZone</code>
Amazon Simple Storage Service (Amazon-S3)	<code>AWS::S3::AccessPoint</code> , <code>AWS::S3::AccountPublicAccessBlock</code> , <code>AWS::S3::Bucket</code> , <code>AWS::S3::MultiRegionAccessPoint</code> , <code>AWS::S3Express::DirectoryBucket</code>
Amazon SageMaker KI	<code>AWS::SageMaker::Model</code> , <code>AWS::SageMaker::NotebookInstance</code>
Amazon-Simple-Notification-Service (Amazon-SNS)	<code>AWS::SNS::Topic</code>
Amazon-Simple-Queue-Service (Amazon SQS)	<code>AWS::SQS::Queue</code>
AWS Secrets Manager	<code>AWS::SecretsManager::Secret</code>
AWS Step Functions	<code>AWS::StepFunctions::StateMachine</code>
AWS Transfer Family	<code>AWS::Transfer::Connector</code>
AWS WAF	<code>AWS::WAF::Rule</code> , <code>AWS::WAF::RuleGroup</code> , <code>AWS::WAF::WebACL</code> , <code>AWS::WAFRegional::Rule</code> , <code>AWS::WAFRegional::RuleGroup</code> , <code>AWS::WAFRegional::WebACL</code> , <code>AWS::WAFv2::RuleGroup</code> , <code>AWS::WAFv2::WebACL</code>
Amazon WorkSpaces	<code>AWS::WorkSpaces::Workspace</code>

Erforderliche Ressourcen für den CIS AWS Foundations Benchmark

Um Sicherheitsüberprüfungen für aktivierte Kontrollen durchzuführen, die für den Center for Internet Security (CIS) AWS Foundations Benchmark gelten, führt Security Hub CSPM entweder genau die für die Prüfungen vorgeschriebenen Prüfschritte durch oder verwendet spezifische AWS Config verwaltete Regeln. Informationen zu diesem Standard in Security Hub CSPM finden Sie unter.

[Benchmark der AWS GUS-Stiftungen im Security Hub CSPM](#)

Erforderliche Ressourcen für CIS v3.0.0

Damit Security Hub CSPM die Ergebnisse für aktivierte, durch Änderungen ausgelöste CIS v3.0.0-Steuererelemente, die eine AWS Config Regel verwenden, korrekt melden kann, müssen Sie die folgenden Ressourcentypen in aufzeichnen. AWS Config

AWS-Service	Ressourcentypen
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::Instance , AWS::EC2::NetworkAcl , AWS::EC2::SecurityGroup
AWS Identity and Access Management (IAM)	AWS::IAM::Group , AWS::IAM::User , AWS::IAM::Role
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBInstance
Amazon Simple Storage Service (Amazon-S3)	AWS::S3::Bucket

Erforderliche Ressourcen für CIS v1.4.0

Damit Security Hub CSPM die Ergebnisse für aktivierte, durch Änderungen ausgelöste CIS v1.4.0-Steuererelemente, die eine AWS Config Regel verwenden, korrekt melden kann, müssen Sie die folgenden Ressourcentypen in aufzeichnen. AWS Config

AWS-Service	Ressourcentypen
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::NetworkAcl , AWS::EC2::SecurityGroup

AWS-Service	Ressourcentypen
AWS Identity and Access Management (IAM)	AWS::IAM::Policy , AWS::IAM::User
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBInstance
Amazon Simple Storage Service (Amazon-S3)	AWS::S3::Bucket

Erforderliche Ressourcen für CIS v1.2.0

Damit Security Hub CSPM die Ergebnisse für aktivierte, durch Änderungen ausgelöste CIS v1.2.0-Steuerelemente, die eine AWS Config Regel verwenden, korrekt melden kann, müssen Sie die folgenden Ressourcentypen in aufzeichnen. AWS Config

AWS-Service	Ressourcentypen
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::SecurityGroup
AWS Identity and Access Management (IAM)	AWS::IAM::Policy , AWS::IAM::User

Erforderliche Ressourcen für den Standard NIST SP 800-53 Revision 5

Damit Security Hub CSPM die Ergebnisse für durch Änderungen ausgelöste Kontrollen, die für den Standard NIST SP 800-53 Revision 5 gelten, aktiviert sind und eine AWS Config Regel verwenden, korrekt melden kann, müssen Sie die folgenden Ressourcentypen in aufzeichnen. AWS Config Informationen zu diesem Standard finden Sie unter. [NIST SP 800-53 Revision 5 im Security Hub CSPM](#)

AWS-Service	Ressourcentypen
Amazon API Gateway	AWS::ApiGateway::Stage , AWS::ApiGatewayV2::Stage
AWS AppSync	AWS::AppSync::GraphQLApi
AWS Backup	AWS::Backup::RecoveryPoint

AWS-Service	Ressourcentypen
AWS Certificate Manager (ACM)	AWS::ACM::Certificate
AWS CloudFormation	AWS::CloudFormation::Stack
Amazon CloudFront	AWS::CloudFront::Distribution
Amazon CloudWatch	AWS::CloudWatch::Alarm
AWS CodeBuild	AWS::CodeBuild::Project
AWS Database Migration Service (AWS DMS)	AWS::DMS::Endpoint , AWS::DMS::ReplicationInstance , AWS::DMS::ReplicationTask
Amazon-DynamoDB	AWS::DynamoDB::Table
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::ClientVpnEndpoint , AWS::EC2::EIP , AWS::EC2::Instance , AWS::EC2::LaunchTemplate , AWS::EC2::NetworkAcl , AWS::EC2::NetworkInterface , AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::TransitGateway , AWS::EC2::VPNConnection , AWS::EC2::Volume
Amazon EC2 Auto Scaling	AWS::AutoScaling::AutoScalingGroup , AWS::AutoScaling::LaunchConfiguration
Amazon Elastic Container Registry (Amazon ECR)	AWS::ECR::Repository
Amazon Elastic Container Service (Amazon ECS)	AWS::ECS::Cluster , AWS::ECS::Service , AWS::ECS::TaskDefinition

AWS-Service	Ressourcentypen
Amazon Elastic File System (Amazon EFS)	<code>AWS::EFS::AccessPoint</code>
Amazon Elastic Kubernetes Service (Amazon EKS)	<code>AWS::EKS::Cluster</code>
AWS Elastic Beanstalk	<code>AWS::ElasticBeanstalk::Environment</code>
Elastic Load Balancing	<code>AWS::ElasticLoadBalancing::LoadBalancer</code> , <code>AWS::ElasticLoadBalancingV2::Listener</code> , <code>AWS::ElasticLoadBalancingV2::LoadBalancer</code>
Amazon ElasticSearch	<code>AWS::Elasticsearch::Domain</code>
Amazon EMR	<code>AWS::EMR::SecurityConfiguration</code>
Amazon EventBridge	<code>AWS::Events::Endpoint</code> , <code>AWS::Events::EventBus</code>
AWS Glue	<code>AWS::Glue::Job</code>
AWS Identity and Access Management (IAM)	<code>AWS::IAM::Group</code> , <code>AWS::IAM::Policy</code> , <code>AWS::IAM::Role</code> , <code>AWS::IAM::User</code>
AWS Key Management Service (AWS KMS)	<code>AWS::KMS::Alias</code> , <code>AWS::KMS::Key</code>
Amazon Kinesis	<code>AWS::Kinesis::Stream</code>
AWS Lambda	<code>AWS::Lambda::Function</code>
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	<code>AWS::MSK::Cluster</code>
Amazon MQ	<code>AWS::AmazonMQ::Broker</code>

AWS-Service	Ressourcentypen
AWS Network Firewall	<code>AWS::NetworkFirewall::Firewall</code> , <code>AWS::NetworkFirewall::FirewallPolicy</code> , <code>AWS::NetworkFirewall::RuleGroup</code>
OpenSearch Amazon-Dienst	<code>AWS::OpenSearch::Domain</code>
Amazon Relational Database Service (Amazon RDS)	<code>AWS::RDS::DBCluster</code> , <code>AWS::RDS::DBClusterSnapshot</code> , <code>AWS::RDS::DBInstance</code> , <code>AWS::RDS::DBSnapshot</code> , <code>AWS::RDS::EventSubscription</code>
Amazon Redshift	<code>AWS::Redshift::Cluster</code> , <code>AWS::Redshift::ClusterSubnetGroup</code>
Amazon Route 53	<code>AWS::Route53::HostedZone</code>
Amazon Simple Storage Service (Amazon-S3)	<code>AWS::S3::AccessPoint</code> , <code>AWS::S3::AccountPublicAccessBlock</code> , <code>AWS::S3::Bucket</code>
AWS Service Catalog	<code>AWS::ServiceCatalog::Portfolio</code>
Amazon-Simple-Notification-Service (Amazon-SNS)	<code>AWS::SNS::Topic</code>
Amazon-Simple-Queue-Service (Amazon SQS)	<code>AWS::SQS::Queue</code>
EC2 Amazon-Systemmanager (SSM)	<code>AWS::SSM::AssociationCompliance</code> , <code>AWS::SSM::ManagedInstanceInventory</code> , <code>AWS::SSM::PatchCompliance</code>
Amazon SageMaker KI	<code>AWS::SageMaker::NotebookInstance</code>
AWS Secrets Manager	<code>AWS::SecretsManager::Secret</code>
AWS Transfer Family	<code>AWS::Transfer::Connector</code>

AWS-Service	Ressourcentypen
AWS WAF	AWS::WAF::Rule , AWS::WAF::RuleGroup , AWS::WAF::WebACL , AWS::WAFRegional::Rule , AWS::WAFRegional::RuleGroup , AWS::WAFRegional::WebACL , AWS::WAFv2::RuleGroup , AWS::WAFv2::WebACL

Erforderliche Ressourcen für den Standard NIST SP 800-171 Revision 2

Damit Security Hub CSPM die Ergebnisse für durch Änderungen ausgelöste Kontrollen, die für den Standard NIST SP 800-171 Revision 2 gelten, aktiviert sind und eine AWS Config Regel verwenden, korrekt melden kann, müssen Sie die folgenden Ressourcentypen in aufzeichnen. AWS Config Informationen zu diesem Standard finden Sie unter. [NIST SP 800-171 Revision 2 im Security Hub CSPM](#)

AWS-Service	Ressourcentypen
AWS Certificate Manager(ACM)	AWS::ACM::Certificate
Amazon API Gateway	AWS::ApiGateway::Stage
Amazon CloudFront	AWS::CloudFront::Distribution
Amazon CloudWatch	AWS::CloudWatch::Alarm
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::ClientVpnEndpoint , AWS::EC2::NetworkAcl , AWS::EC2::SecurityGroup , AWS::EC2::VPC , AWS::EC2::VPNConnection
Elastic Load Balancing	AWS::ElasticLoadBalancing::LoadBalancer
AWS Identity and Access Management(IAM)	AWS::IAM::Policy , AWS::IAM::User
AWS Key Management Service (AWS KMS)	AWS::KMS::Alias , AWS::KMS::Key

AWS-Service	Ressourcentypen
AWS Network Firewall	<code>AWS::NetworkFirewall::FirewallPolicy</code> , <code>AWS::NetworkFirewall::RuleGroup</code>
Amazon Simple Storage Service (Amazon S3)	<code>AWS::S3::Bucket</code>
Amazon Simple Notification Service (Amazon SNS)	<code>AWS::SNS::Topic</code>
AWS Systems Manager(SSM)	<code>AWS::SSM::PatchCompliance</code>
AWS WAF	<code>AWS::WAFv2::RuleGroup</code>

Erforderliche Ressourcen für PCI DSS v3.2.1

Damit Security Hub CSPM die Ergebnisse für Kontrollen, die für Version 3.2.1 des Payment Card Industry Data Security Standard (PCI DSS) gelten, aktiviert sind und eine AWS Config Regel verwenden, korrekt melden kann, müssen Sie die folgenden Ressourcentypen in aufzeichnen. AWS Config Informationen zu diesem Standard finden Sie unter [PCI DSS im Security Hub CSPM](#)

AWS-Service	Ressourcentypen
AWS CodeBuild	<code>AWS::CodeBuild::Project</code>
Amazon Elastic Compute Cloud (Amazon EC2)	<code>AWS::EC2::EIP</code> , <code>AWS::EC2::Instance</code> , <code>AWS::EC2::SecurityGroup</code>
Amazon EC2 Auto Scaling	<code>AWS::AutoScaling::AutoScalingGroup</code>
AWS Identity and Access Management (IAM)	<code>AWS::IAM::Policy</code> , <code>AWS::IAM::User</code>
AWS Lambda	<code>AWS::Lambda::Function</code>
OpenSearch Amazon-Dienst	<code>AWS::OpenSearch::Domain</code>

AWS-Service	Ressourcentypen
Amazon Relational Database Service (Amazon RDS)	<code>AWS::RDS::DBClusterSnapshot</code> , <code>AWS::RDS::DBInstance</code> , <code>AWS::RDS::DBSnapshot</code>
Amazon Redshift	<code>AWS::Redshift::Cluster</code>
Amazon Simple Storage Service (Amazon-S3)	<code>AWS::S3::AccountPublicAccessBlock</code> , <code>AWS::S3::Bucket</code>
EC2 Amazon-Systemmanager (SSM)	<code>AWS::SSM::AssociationCompliance</code> , <code>AWS::SSM::ManagedInstanceInventory</code> , <code>AWS::SSM::PatchCompliance</code>

Erforderliche Ressourcen für den AWS Resource Tagging-Standard

Alle Steuerelemente, die für den AWS Resource Tagging-Standard gelten, werden durch Änderungen ausgelöst und verwenden eine AWS Config Regel. Damit Security Hub CSPM die Ergebnisse dieser Kontrollen korrekt melden kann, müssen Sie die folgenden Ressourcentypen in aufzeichnen. AWS Config Informationen zu diesem Standard finden Sie unter [AWS Standard für Ressourcen-Tagging in Security Hub CSPM](#)

AWS-Service	Ressourcentypen
AWS Amplify	<code>AWS::Amplify::App</code> , <code>AWS::Amplify::Branch</code>
Amazon AppFlow	<code>AWS::AppFlow::Flow</code>
AWS App Runner	<code>AWS::AppRunner::Service</code> , <code>AWS::AppRunner::VpcConnector</code>
AWS AppConfig	<code>AWS::AppConfig::Application</code> , <code>AWS::AppConfig::ConfigurationProfile</code> , <code>AWS::AppConfig::En</code>

AWS-Service	Ressourcentypen
	<code>Environment</code> , <code>AWS::AppConfig::ExtensionAssociation</code>
AWS AppSync	<code>AWS::AppSync::GraphQLApi</code>
Amazon Athena	<code>AWS::Athena::DataCatalog</code> , <code>AWS::Athena::WorkGroup</code>
AWS Backup	<code>AWS::Backup::BackupPlan</code> , <code>AWS::Backup::BackupVault</code> , <code>AWS::Backup::RecoveryPlan</code> , <code>AWS::Backup::ReportPlan</code>
AWS Batch	<code>AWS::Batch::ComputeEnvironment</code> , <code>AWS::Batch::JobQueue</code> , <code>AWS::Batch::SchedulingPolicy</code>
AWS Certificate Manager (ACM)	<code>AWS::ACM::Certificate</code>
AWS CloudFormation	<code>AWS::CloudFormation::Stack</code>
Amazon CloudFront	<code>AWS::CloudFront::Distribution</code>
AWS CloudTrail	<code>AWS::CloudTrail::Trail</code>
AWS CodeArtifact	<code>AWS::CodeArtifact::Repository</code>
Amazon CodeGuru	<code>AWS::CodeGuruProfiler::ProfilingGroup</code> , <code>AWS::CodeGuruReviewer::RepositoryAssociation</code>
Amazon Connect	<code>AWS::CustomerProfiles::ObjectType</code>

AWS-Service	Ressourcentypen
AWS Database Migration Service (AWS DMS)	<code>AWS::DMS::Certificate</code> , <code>AWS::DMS::EventSubscription</code> <code>AWS::DMS::ReplicationInstance</code> , <code>AWS::DMS::ReplicationSubnetGroup</code>
AWS DataSync	<code>AWS::DataSync::Task</code>
Amazon Detective	<code>AWS::Detective::Graph</code>
Amazon-DynamoDB	<code>AWS::DynamoDB::Trail</code>
Amazon Elastic Compute Cloud (EC2)	<code>AWS::EC2::CustomerGateway</code> , <code>AWS::EC2::DHCPOptions</code> , <code>AWS::EC2::EIP</code> , <code>AWS::EC2::FlowLog</code> , <code>AWS::EC2::Instance</code> , <code>AWS::EC2::InternetGateway</code> , <code>AWS::EC2::LaunchTemplate</code> , <code>AWS::EC2::NatGateway</code> , <code>AWS::EC2::NetworkAcl</code> , <code>AWS::EC2::NetworkInterface</code> , <code>AWS::EC2::PrefixList</code> , <code>AWS::EC2::RouteTable</code> , <code>AWS::EC2::SecurityGroup</code> , <code>AWS::EC2::Subnet</code> , <code>AWS::EC2::TrafficMirrorFilter</code> , <code>AWS::EC2::TrafficMirrorSession</code> , <code>AWS::EC2::TrafficMirrorTarget</code> , <code>AWS::EC2::TransitGateway</code> , <code>AWS::EC2::TransitGatewayAttachment</code> , <code>AWS::EC2::TransitGatewayRouteTable</code> , <code>AWS::EC2::Volume</code> , <code>AWS::EC2::VPC</code> , <code>AWS::EC2::VPCEndpointService</code> , <code>AWS::EC2::VPCPeeringConnection</code> , <code>AWS::EC2::VPNGateway</code>

AWS-Service	Ressourcentypen
Amazon EC2 Auto Scaling	<code>AWS::AutoScaling::AutoScalingGroup</code>
Amazon Elastic Container Registry (Amazon ECR)	<code>AWS::ECR::PublicRepository</code>
Amazon Elastic Container Service (Amazon ECS)	<code>AWS::ECS::Cluster</code> , <code>AWS::ECS::Service</code> , <code>AWS::ECS::TaskDefinition</code>
Amazon Elastic File System (Amazon EFS)	<code>AWS::EFS::AccessPoint</code>
Amazon Elastic Kubernetes Service (Amazon EKS)	<code>AWS::EKS::Cluster</code> , <code>AWS::EKS::IdentityProviderConfig</code>
AWS Elastic Beanstalk	<code>AWS::ElasticBeanstalk::Environment</code>
ElasticSearch	<code>AWS::Elasticsearch::Domain</code>
Amazon EventBridge	<code>AWS::Events::EventBus</code>
Amazon Fraud Detector	<code>AWS::FraudDetector::EntityType</code> , <code>AWS::FraudDetector::Label</code> <code>AWS::FraudDetector::Outcome</code> , <code>AWS::FraudDetector::Variable</code>
AWS Global Accelerator	<code>AWS::GlobalAccelerator::Accelerator</code>
AWS Glue	<code>AWS::Glue::Job</code>
Amazon GuardDuty	<code>AWS::GuardDuty::Detector</code> , <code>AWS::GuardDuty::Filter</code> , <code>AWS::GuardDuty::IPSet</code>

AWS-Service	Ressourcentypen
AWS Identity and Access Management (IAM)	AWS::IAM::Role , AWS::IAM::User
AWS Identity and Access Management Access Analyzer (IAM-Zugriffsanalysator)	AWS::AccessAnalyzer::Analyzer
AWS IoT	AWS::IoT::Authorizer , AWS::IoT::Dimension , AWS::IoT::MitigationAction , AWS::IoT::Policy , AWS::IoT::RoleAlias , AWS::IoT::SecurityProfile
AWS IoT Events	AWS::IoTEvents::AlarmModel , AWS::IoTEvents::DetectorModel , AWS::IoTEvents::Input
AWS IoT SiteWise	AWS::IoTSiteWise::Dashboard , AWS::IoTSiteWise::Gateway , AWS::IoTSiteWise::Portal , AWS::IoTSiteWise::Project
AWS IoT TwinMaker	AWS::IoTTwinMaker::Entity , AWS::IoTTwinMaker::Scene , AWS::IoTTwinMaker::SyncJob , AWS::IoTTwinMaker::Workspace
AWS IoT Drahtlos	AWS::IoTWireless::FirmwareTask , AWS::IoTWireless::MulticastGroup , AWS::IoTWireless::ServiceProfile
Amazon Interactive Video Service (Amazon IVS)	AWS::IVS::Channel , AWS::IVS::PlaybackKeyPair , AWS::IVS::RecordingConfiguration
Amazon Keyspaces (für Apache Cassandra)	AWS::Cassandra::Keyspace

AWS-Service	Ressourcentypen
Amazon Kinesis	AWS::Kinesis::Stream
AWS Lambda	AWS::Lambda::Function
Amazon MQ	AWS::AmazonMQ::Broker
AWS Network Firewall	AWS::NetworkFirewall::Firewall , AWS::NetworkFirewall::FirewallPolicy
OpenSearch Amazon-Dienst	AWS::OpenSearch::Domain
AWS Private Certificate Authority	AWS::ACMPCA::CertificateAuthority
Amazon Relational Database Service	AWS::RDS::DBCluster , AWS::RDS::DBClusterSnapshot , AWS::RDS::DBInstance , AWS::RDS::DBSecurityGroup , AWS::RDS::DBSnapshot , AWS::RDS::DBSubnetGroup
Amazon Redshift	AWS::Redshift::Cluster , AWS::Redshift::ClusterParameterGroup , AWS::Redshift::ClusterSnapshot , AWS::Redshift::ClusterSubnetGroup , AWS::Redshift::EventSubscription
Amazon Route 53	AWS::Route53::HealthCheck
Amazon SageMaker KI	AWS::SageMaker::AppImageConfig , AWS::SageMaker::Image
AWS Secrets Manager	AWS::SecretsManager::Secret
Amazon Simple Email Service (Amazon SES)	AWS::SES::ConfigurationSet , AWS::SES::ContactList

AWS-Service	Ressourcentypen
Amazon Simple Notification Service (Amazon SNS)	<code>AWS::SNS::Topic</code>
Amazon-Simple-Queue-Service (Amazon SQS)	<code>AWS::SQS::Queue</code>
AWS Step Functions	<code>AWS::StepFunctions::Activity</code>
AWS Systems Manager (SSM)	<code>AWS::SSM::Document</code>
AWS Transfer Family	<code>AWS::Transfer::Agreement</code> , <code>AWS::Transfer::Certificate</code> , <code>AWS::Transfer::Connector</code> , <code>AWS::Transfer::Profile</code> , <code>AWS::Transfer::Workflow</code>

Erforderliche Ressourcen für den AWS Control Tower Service-Managed-Standard

Damit Security Hub CSPM die Ergebnisse für durch Änderungen ausgelöste Kontrollen, die für den AWS Control Tower Service-Managed-Standard gelten, aktiviert sind und eine AWS Config Regel verwenden, korrekt meldet, müssen Sie die folgenden Ressourcentypen in aufzeichnen. AWS Config Informationen zu diesem Standard finden Sie unter. [Vom Service verwalteter Standard: AWS Control Tower](#)

AWS-Service	Ressourcentypen
Amazon API Gateway	<code>AWS::ApiGateway::Stage</code> <code>AWS::ApiGatewayV2::Stage</code>
AWS Certificate Manager (ACM)	<code>AWS::ACM::Certificate</code>
AWS CodeBuild	<code>AWS::CodeBuild::Project</code>
Amazon-DynamoDB	<code>AWS::DynamoDB::Table</code>
Amazon Elastic Compute Cloud (EC2)	<code>AWS::EC2::Instance</code>

AWS-Service	Ressourcentypen
	AWS::EC2::NetworkAcl AWS::EC2::NetworkInterface AWS::EC2::SecurityGroup AWS::EC2::Subnet AWS::EC2::VPNConnection AWS::EC2::Volume
Amazon EC2 Auto Scaling	AWS::AutoScaling::AutoScalingGroup AWS::AutoScaling::LaunchConfiguration
Amazon Elastic Container Registry (Amazon ECR)	AWS::ECR::Repository
Amazon Elastic Container Service (Amazon ECS)	AWS::ECS::Cluster AWS::ECS::Service AWS::ECS::TaskDefinition
Amazon Elastic File System (Amazon EFS)	AWS::EFS::AccessPoint
Amazon EKS	AWS::EKS::Cluster
ElasticBeanstalk	AWS::ElasticBeanstalk::Environment
Elastic Load Balancing	AWS::ElasticLoadBalancing::LoadBalancer AWS::ElasticLoadBalancingV2::LoadBalancer

AWS-Service	Ressourcentypen
ElasticSearch	AWS::Elasticsearch::Domain
AWS Identity and Access Management (IAM)	AWS::IAM::Group AWS::IAM::Policy AWS::IAM::Role AWS::IAM::User
AWS Key Management Service (AWS KMS)	AWS::KMS::Alias AWS::KMS::Key
Amazon Kinesis	AWS::Kinesis::Stream
AWS Lambda	AWS::Lambda::Function
AWS Network Firewall	AWS::NetworkFirewall::FirewallPolicy AWS::NetworkFirewall::RuleGroup
OpenSearch Amazon-Dienst	AWS::OpenSearch::Domain
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBCluster AWS::RDS::DBClusterSnapshot AWS::RDS::DBInstance AWS::RDS::DBSnapshot AWS::RDS::EventSubscription
Amazon Redshift	AWS::Redshift::Cluster

AWS-Service	Ressourcentypen
Amazon Simple Storage Service (Amazon-S3)	AWS::S3::AccountPublicAccessBlock AWS::S3::Bucket
Amazon-Simple-Notification-Service (Amazon-SNS)	AWS::SNS::Topic
Amazon-Simple-Queue-Service (Amazon SQS)	AWS::SQS::Queue
AWS Secrets Manager	AWS::SecretsManager::Secret
EC2 Amazon-Systemmanager (SSM)	AWS::SSM::AssociationCompliance AWS::SSM::ManagedInstanceInventory AWS::SSM::PatchCompliance
AWS WAF	AWS::WAFRegional::Rule AWS::WAFRegional::RuleGroup AWS::WAFRegional::WebACL AWS::WAFv2::WebACL

Zeitplan für die Ausführung von Sicherheitsprüfungen

Nachdem Sie einen Sicherheitsstandard aktiviert haben, beginnt AWS Security Hub Cloud Security Posture Management (CSPM), alle Prüfungen innerhalb von zwei Stunden durchzuführen. Die meisten Prüfungen werden innerhalb von 25 Minuten ausgeführt. Security Hub CSPM führt Prüfungen durch, indem es die Regel auswertet, die einer Kontrolle zugrunde liegt. Bis ein Steuerelement seinen ersten Prüflauf abgeschlossen hat, lautet sein Status Keine Daten.

Wenn Sie einen neuen Standard aktivieren, kann es bis zu 24 Stunden dauern, bis Security Hub CSPM Ergebnisse für Kontrollen generiert, die dieselbe zugrunde liegende AWS Config serviceverknüpfte Regel verwenden wie aktivierte Steuerelemente aus anderen aktivierten

Standards. Wenn Sie beispielsweise das [Lambda.1-Steuerelement](#) im Standard AWS Foundation Security Best Practices (FSBP) aktivieren, erstellt Security Hub CSPM die serviceverknüpfte Regel und generiert Ergebnisse in der Regel innerhalb von Minuten. Wenn Sie danach das Lambda.1-Steuerelement im Payment Card Industry Data Security Standard (PCI DSS) aktivieren, kann es bis zu 24 Stunden dauern, bis Security Hub CSPM Ergebnisse für die Kontrolle generiert, da es dieselbe serviceverknüpfte Regel verwendet.

Nach der ersten Überprüfung kann der Zeitplan für jede Kontrolle entweder periodisch oder durch Änderungen ausgelöst werden. Für ein Steuerelement, das auf einer verwalteten AWS Config Regel basiert, enthält die Beschreibung des Steuerelements einen Link zur Regelbeschreibung im AWS Config Entwicklerhandbuch. Diese Beschreibung gibt an, ob es sich bei der Regel um eine Änderung handelt oder ob sie regelmäßig geändert wird.

Regelmäßige Sicherheitsüberprüfungen

Regelmäßige Sicherheitsüberprüfungen werden automatisch innerhalb von 12 oder 24 Stunden nach der letzten Ausführung ausgeführt. Security Hub CSPM bestimmt die Periodizität, und Sie können sie nicht ändern. Bei regelmäßigen Kontrollen erfolgt die Bewertung zu dem Zeitpunkt, zu dem die Prüfung ausgeführt wird.

Wenn Sie den Workflow-Status eines periodischen Kontrollbefundes aktualisieren und dann bei der nächsten Überprüfung der Konformitätsstatus des Ergebnisses unverändert bleibt, bleibt der Workflow-Status in seinem geänderten Status. Wenn Sie beispielsweise eine fehlerhafte Suche für das [KMS.4-Steuerelement](#) haben (die AWS KMS key Rotation sollte aktiviert sein) und das Ergebnis anschließend korrigieren, ändert Security Hub CSPM den Workflow-Status von zu. NEW RESOLVED Wenn Sie die KMS-Schlüsselrotation vor der nächsten regelmäßigen Überprüfung deaktivieren, bleibt der Workflow-Status des Ergebnisses erhalten. RESOLVED

Prüfungen, die benutzerdefinierte Lambda-Funktionen von Security Hub CSPM verwenden, werden regelmäßig durchgeführt.

Durch Änderungen ausgelöste Sicherheitsüberprüfungen

Durch Änderungen ausgelöste Sicherheitsüberprüfungen werden ausgeführt, wenn sich der Status der zugehörigen Ressource ändert. AWS Config ermöglicht es Ihnen, zwischen der kontinuierlichen Aufzeichnung von Änderungen des Ressourcenstatus und der täglichen Aufzeichnung zu wählen. Wenn Sie die tägliche Aufzeichnung wählen AWS Config , werden die Ressourcenkonfigurationsdaten am Ende jedes 24-Stunden-Zeitraums bereitgestellt, wenn sich der Ressourcenstatus ändert. Wenn es keine Änderungen gibt, werden keine Daten geliefert. Dies kann

die Generierung von Security Hub CSPM-Ergebnissen verzögern, bis ein Zeitraum von 24 Stunden abgeschlossen ist. Unabhängig von Ihrem gewählten Aufzeichnungszeitraum überprüft Security Hub CSPM alle 18 Stunden, ob keine Ressourcen-Updates von verpasst AWS Config wurden.

Im Allgemeinen verwendet Security Hub CSPM wann immer möglich durch Änderungen ausgelöste Regeln. Damit eine Ressource eine durch Änderungen ausgelöste Regel verwenden kann, muss sie Konfigurationselemente unterstützen. AWS Config

Generierung und Aktualisierung von Kontrollbefunden

AWS Security Hub Cloud Security Posture Management (CSPM) generiert und aktualisiert Kontrollergebnisse, wenn es Prüfungen anhand von Sicherheitskontrollen durchführt. Die Kontrollergebnisse verwenden das [AWS Security Finding Format \(ASFF\)](#).

Security Hub CSPM berechnet normalerweise Gebühren für jede Sicherheitsüberprüfung für eine Kontrolle. Wenn jedoch mehrere Kontrollen dieselbe AWS Config Regel verwenden, berechnet Security Hub CSPM für jede Überprüfung anhand der Regel nur einmal eine Gebühr. Die AWS Config `iam-password-policy` Regel wird beispielsweise von mehreren Kontrollen im CIS AWS Foundations Benchmark-Standard und im AWS Foundational Security Best Practices-Standard verwendet. Jedes Mal, wenn Security Hub CSPM eine Überprüfung anhand dieser Regel durchführt, generiert es ein separates Kontrollergebnis für jede zugehörige Kontrolle, berechnet jedoch nur einmal für die Prüfung eine Gebühr.

Wenn die Größe eines Kontrollergebnisses das Maximum von 240 KB überschreitet, entfernt Security Hub CSPM das `Resource.Details` Objekt aus dem Befund. Bei Kontrollen, die durch AWS Config Ressourcen unterstützt werden, können Sie die Ressourcendetails mithilfe der AWS Config Konsole überprüfen.

Themen

- [Konsolidierte Kontrollergebnisse](#)
- [Generierung, Aktualisierung und Archivierung von Kontrollbefunden](#)
- [Automatisierung und Unterdrückung von Kontrollbefunden](#)
- [Einzelheiten zur Einhaltung der Kontrollbestimmungen](#)
- [ProductFields Einzelheiten zu den Kontrollbefunden](#)
- [Schweregrade der Kontrollbefunde](#)

Konsolidierte Kontrollergebnisse

Wenn konsolidierte Kontrollergebnisse für Ihr Konto aktiviert sind, generiert Security Hub CSPM für jede Sicherheitsüberprüfung einer Kontrolle ein einzelnes Ergebnis oder ein einzelnes Befundupdate, auch wenn eine Kontrolle für mehrere aktivierte Standards gilt. Eine Liste der Kontrollen und der Standards, für die sie gelten, finden Sie unter [Kontrollreferenz für Security Hub CSPM](#). Wir empfehlen, konsolidierte Kontrollergebnisse zu aktivieren, um das Störgeräusch zu reduzieren.

Wenn Sie Security Hub CSPM AWS-Konto vor dem 23. Februar 2023 aktiviert haben, können Sie konsolidierte Kontrollergebnisse aktivieren, indem Sie den Anweisungen weiter unten in diesem Abschnitt folgen. Wenn Sie Security Hub CSPM am oder nach dem 23. Februar 2023 aktivieren, werden die konsolidierten Kontrollergebnisse automatisch für Ihr Konto aktiviert.

Wenn Sie die [Security Hub CSPM-Integration mit](#) Mitgliedskonten verwenden AWS Organizations oder Mitgliedskonten über einen [manuellen Einladungsprozess](#) eingeladen haben, ist Consolidated Control Findings nur dann für Mitgliedskonten aktiviert, wenn sie für das Administratorkonto aktiviert ist. Wenn die Funktion für das Administratorkonto deaktiviert ist, ist sie auch für Mitgliedskonten deaktiviert. Dieses Verhalten gilt für neue und bestehende Mitgliedskonten. Wenn der Administrator die [zentrale Konfiguration](#) verwendet, um Security Hub CSPM für mehrere Konten zu verwalten, kann er außerdem keine zentralen Konfigurationsrichtlinien verwenden, um konsolidierte Kontrollergebnisse für die Konten zu aktivieren oder zu deaktivieren.

Wenn Sie konsolidierte Kontrollergebnisse für Ihr Konto deaktivieren, generiert oder aktualisiert Security Hub CSPM ein separates Kontrollergebnis für jeden aktivierten Standard, der eine Kontrolle enthält. Wenn Sie beispielsweise vier Standards aktivieren, die sich eine Kontrolle teilen, erhalten Sie nach einer Sicherheitsüberprüfung für die Kontrolle vier separate Ergebnisse. Wenn Sie konsolidierte Kontrollergebnisse aktivieren, erhalten Sie nur ein Ergebnis.

Wenn Sie konsolidierte Kontrollergebnisse aktivieren, erstellt Security Hub CSPM neue standardunabhängige Ergebnisse und archiviert die ursprünglichen standardbasierten Ergebnisse. Einige Felder und Werte für Kontrollergebnisse werden sich ändern, was sich auf Ihre bestehenden Workflows auswirken kann. Informationen zu diesen Änderungen finden Sie unter [Konsolidierte Kontrollergebnisse — ASFF-Änderungen](#). Die Aktivierung konsolidierter Kontrollergebnisse kann sich auch auf die Ergebnisse auswirken, die integrierte Drittanbieterprodukte von Security Hub CSPM erhalten. Wenn Sie die Lösung [Automated Security Response auf AWS Version 2.0.0](#) verwenden, beachten Sie, dass sie konsolidierte Kontrollergebnisse unterstützt.

Um Consolidated Control Findings zu aktivieren oder zu deaktivieren, müssen Sie mit einem Administratorkonto oder einem eigenständigen Konto angemeldet sein.

 Note

Nachdem Sie die konsolidierten Kontrollergebnisse aktiviert haben, kann es bis zu 24 Stunden dauern, bis Security Hub CSPM neue konsolidierte Ergebnisse generiert und die vorhandenen standardbasierten Ergebnisse archiviert hat. Ebenso kann es nach der Deaktivierung konsolidierter Kontrollergebnisse bis zu 24 Stunden dauern, bis Security Hub CSPM neue standardbasierte Ergebnisse generiert und die vorhandenen konsolidierten Ergebnisse archiviert hat. In diesen Zeiten kann es sein, dass Sie in Ihrem Konto eine Mischung aus standardunabhängigen und standardbasierten Ergebnissen sehen.

Security Hub CSPM console

Um konsolidierte Kontrollergebnisse zu aktivieren oder zu deaktivieren

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>
2. Klicken Sie im Navigationsbereich unter Settings auf General.
3. Wählen Sie im Bereich Controls die Option Bearbeiten aus.
4. Verwenden Sie den Schalter Konsolidierte Kontrollergebnisse, um konsolidierte Kontrollergebnisse zu aktivieren oder zu deaktivieren.
5. Wählen Sie Speichern.

Security Hub CSPM API

Verwenden Sie den [UpdateSecurityHubConfiguration](#) Betrieb der Security Hub CSPM-API, um konsolidierte Kontrollergebnisse programmgesteuert zu aktivieren oder zu deaktivieren. Oder, wenn Sie den verwenden, führen Sie den Befehl aus AWS CLI. [update-security-hub-configuration](#)

Geben Sie für den `control-finding-generator` Parameter `SECURITY_CONTROL` an, ob konsolidierte Kontrollergebnisse aktiviert werden sollen. Geben Sie an, um konsolidierte Kontrollergebnisse zu deaktivieren `STANDARD_CONTROL`.

Mit dem folgenden AWS CLI Befehl werden beispielsweise konsolidierte Kontrollbefunde aktiviert.

```
$ aws securityhub --region us-east-1 update-security-hub-configuration --control-finding-generator SECURITY_CONTROL
```

Mit dem folgenden AWS CLI Befehl werden konsolidierte Kontrollergebnisse deaktiviert.

```
$ aws securityhub --region us-east-1 update-security-hub-configuration --control-finding-generator STANDARD_CONTROL
```

Generierung, Aktualisierung und Archivierung von Kontrollbefunden

[Security Hub CSPM führt Sicherheitsüberprüfungen nach einem Zeitplan durch.](#) Wenn Security Hub CSPM zum ersten Mal eine Sicherheitsüberprüfung für ein Steuerelement durchführt, generiert es für jede AWS Ressource, die das Steuerelement überprüft, ein neues Ergebnis. Jedes Mal, wenn Security Hub CSPM anschließend eine Sicherheitsüberprüfung für die Kontrolle durchführt, aktualisiert es die vorhandenen Ergebnisse, um die Ergebnisse der Prüfung zu melden. Das bedeutet, dass Sie anhand der Daten einzelner Ergebnisse die Konformität bestimmter Ressourcen anhand bestimmter Kontrollen nachverfolgen können.

Wenn sich beispielsweise der Konformitätsstatus einer Ressource PASSED für eine bestimmte Kontrolle von FAILED zu ändert, generiert Security Hub CSPM kein neues Ergebnis. Stattdessen aktualisiert Security Hub CSPM die vorhandenen Ergebnisse für das Steuerelement und die Ressource. In diesem Ergebnis ändert Security Hub CSPM den Wert für das Feld Compliance-Status (Compliance.Status) auf PASSED. Security Hub CSPM aktualisiert auch die Werte für zusätzliche Felder, um die Ergebnisse der Prüfung widerzuspiegeln, z. B. den Schweregrad, den Workflow-Status und Zeitstempel, die angeben, wann Security Hub CSPM die Prüfung zuletzt ausgeführt und das Ergebnis aktualisiert hat.

Bei der Meldung von Änderungen des Compliance-Status aktualisiert Security Hub CSPM möglicherweise eines der folgenden Felder in einem Kontrollergebnis:

- **Compliance.Status**— Der neue Konformitätsstatus der Ressource für die angegebene Kontrolle.
- **FindingProviderFields.Severity.Label**— Die neue qualitative Darstellung des Schweregrads des Befundes, z. B. LOWMEDIUM, oder HIGH.
- **FindingProviderFields.Severity.Original**— Die neue quantitative Darstellung des Schweregrads des Fehlers, z. B. 0 für eine konforme Ressource.
- **FirstObservedAt**— Wann sich der Konformitätsstatus der Ressource zuletzt geändert hat.
- **LastObservedAt**— Wann Security Hub CSPM die Sicherheitsüberprüfung für das angegebene Steuerelement und die angegebene Ressource zuletzt ausgeführt hat.

- `ProcessedAt`— Wann Security Hub CSPM zuletzt mit der Verarbeitung des Ergebnisses begann.
- `ProductFields.PreviousComplianceStatus`— Der vorherige Konformitätsstatus (`Compliance.Status`) der Ressource für die angegebene Kontrolle.
- `UpdatedAt`— Wann Security Hub CSPM das Ergebnis zuletzt aktualisiert hat.
- `Workflow.Status`— Der Stand der Untersuchung des Ergebnisses, basierend auf dem neuen Konformitätsstatus der Ressource für die angegebene Kontrolle.

Ob Security Hub CSPM ein Feld aktualisiert, hängt in erster Linie von den Ergebnissen der letzten Sicherheitsprüfung für die entsprechende Kontrolle und Ressource ab. Wenn sich beispielsweise der Konformitätsstatus einer Ressource `FAILED` für eine bestimmte Kontrolle von `PASSED` zu ändert, ändert Security Hub CSPM den Workflow-Status des Ergebnisses auf `NEW`. Um Aktualisierungen einzelner Ergebnisse nachzuverfolgen, können Sie auf die Historie eines Befundes zurückgreifen. Einzelheiten zu einzelnen Feldern in Ergebnissen finden Sie unter [AWS Security Finding Format \(ASFF\)](#).

In bestimmten Fällen generiert Security Hub CSPM neue Ergebnisse für nachfolgende Prüfungen durch eine Kontrolle, anstatt bestehende Ergebnisse zu aktualisieren. Dies kann der Fall sein, wenn ein Problem mit der AWS Config Regel vorliegt, die ein Steuerelement unterstützt. In diesem Fall archiviert Security Hub CSPM den vorhandenen Befund und generiert für jede Prüfung einen neuen Befund. In den neuen Ergebnissen lautet der Compliance-Status `NOT_AVAILABLE` und der Datensatzstatus lautet `ARCHIVED`. Nachdem Sie das Problem mit der AWS Config Regel behoben haben, generiert Security Hub CSPM neue Ergebnisse und beginnt, diese zu aktualisieren, um nachfolgende Änderungen am Compliance-Status einzelner Ressourcen nachzuverfolgen.

Security Hub CSPM generiert und aktualisiert nicht nur Kontrollergebnisse, sondern archiviert auch automatisch Kontrollergebnisse, die bestimmte Kriterien erfüllen. Security Hub CSPM archiviert einen Befund, wenn das Steuerelement deaktiviert ist, die angegebene Ressource gelöscht wurde oder die angegebene Ressource nicht mehr existiert. Eine Ressource ist möglicherweise nicht mehr vorhanden, da der zugehörige Dienst nicht mehr verwendet wird. Insbesondere archiviert Security Hub CSPM automatisch ein Kontrollergebnis, wenn das Ergebnis eines der folgenden Kriterien erfüllt:

- Das Ergebnis wurde seit 3-5 Tagen nicht aktualisiert. Beachten Sie, dass die Archivierung auf der Grundlage dieses Zeitrahmens nach bestem Wissen und Gewissen erfolgt und nicht garantiert werden kann.
- `NOT_APPLICABLE` Bei der zugehörigen AWS Config Bewertung wurde der Konformitätsstatus der angegebenen Ressource ermittelt.

Um festzustellen, ob ein Ergebnis archiviert ist, können Sie im Feld Datensatzstatus (RecordState) des Ergebnisses nachschlagen. Wenn ein Ergebnis archiviert ist, lautet der Wert für dieses Feld ARCHIVED.

Security Hub CSPM speichert archivierte Kontrollbefunde 30 Tage lang. Nach 30 Tagen laufen die Ergebnisse ab und Security Hub CSPM löscht sie dauerhaft. Um festzustellen, ob ein archiviertes Kontrollergebnis abgelaufen ist, stützt Security Hub CSPM seine Berechnung auf den Wert für das UpdatedAt Feld des Ergebnisses.

Um archivierte Kontrollergebnisse für mehr als 30 Tage zu speichern, können Sie die Ergebnisse in einen S3-Bucket exportieren. Sie können dies tun, indem Sie eine benutzerdefinierte Aktion mit einer EventBridge Amazon-Regel verwenden. Weitere Informationen finden Sie unter [Verwendung EventBridge für automatisierte Reaktionen und Problembehebungen](#).

Note

Vor dem 3. Juli 2025 generierte und aktualisierte Security Hub CSPM Kontrollergebnisse unterschiedlich, wenn sich der Compliance-Status einer Ressource für eine Kontrolle änderte. Zuvor hat Security Hub CSPM einen neuen Kontrollbefund erstellt und den vorhandenen Befund für eine Ressource archiviert. Daher haben Sie möglicherweise mehrere archivierte Ergebnisse für eine bestimmte Kontrolle und Ressource, bis diese Ergebnisse ablaufen (nach 30 Tagen).

Automatisierung und Unterdrückung von Kontrollbefunden

Sie können die CSPM-Automatisierungsregeln von Security Hub verwenden, um bestimmte Kontrollergebnisse zu aktualisieren oder zu unterdrücken. Wenn Sie ein Ergebnis unterdrücken, können Sie weiterhin darauf zugreifen. Eine Unterdrückung deutet jedoch darauf hin, dass Sie der Meinung sind, dass keine Maßnahmen erforderlich sind, um das Ergebnis zu beheben.

Durch das Unterdrücken von Ergebnissen können Sie das Suchrauschen reduzieren. Sie können beispielsweise Kontrollergebnisse unterdrücken, die in Testkonten generiert wurden. Oder Sie könnten Ergebnisse unterdrücken, die sich auf bestimmte Ressourcen beziehen. Weitere Informationen zur automatischen Aktualisierung oder Unterdrückung von Ergebnissen finden Sie unter [Grundlegendes zu den Automatisierungsregeln in Security Hub CSPM](#).

Automatisierungsregeln eignen sich, wenn Sie bestimmte Kontrollergebnisse aktualisieren oder unterdrücken möchten. Wenn ein Steuerelement jedoch für Ihre Organisation oder Ihren

Anwendungsfall nicht relevant ist, empfehlen wir, [das Steuerelement zu deaktivieren](#). Wenn Sie eine Kontrolle deaktivieren, führt Security Hub CSPM keine Sicherheitsprüfungen für sie durch und es werden Ihnen keine Gebühren dafür berechnet.

Einzelheiten zur Einhaltung der Kontrollbestimmungen

Bei Ergebnissen, die durch Sicherheitsprüfungen für Kontrollen generiert wurden, enthalten das [Compliance-Objekt](#) und die Felder im AWS Security Finding Format (ASFF) Konformitätsdetails für einzelne Ressourcen, die von einer Kontrolle überprüft wurden. Dazu gehören die folgenden Informationen:

- **AssociatedStandards**— Die aktivierten Standards, in denen das Steuerelement aktiviert ist.
- **RelatedRequirements**— Die entsprechenden Anforderungen für die Steuerung in allen aktivierten Standards. Diese Anforderungen ergeben sich aus Sicherheits-Frameworks von Drittanbietern für die Steuerung, wie dem Payment Card Industry Data Security Standard (PCI DSS) oder dem Standard NIST SP 800-171 Revision 2.
- **SecurityControlId**— Die Kennung für die Steuerung aller Standards, die Security Hub CSPM unterstützt.
- **Status**— Das Ergebnis der letzten Überprüfung, die Security Hub CSPM für die Kontrolle durchgeführt hat. Die Ergebnisse früherer Prüfungen werden in der Befundhistorie gespeichert.
- **StatusReasons**— Ein Array, das die Gründe für den durch das Status Feld angegebenen Wert auflistet. Für jeden Grund enthält dies einen Ursachencode und eine Beschreibung.

In der folgenden Tabelle sind Ursachencodes und Beschreibungen aufgeführt, die ein Ergebnis in der StatusReasons Matrix enthalten könnte. Die Behebungsschritte hängen davon ab, welche Kontrolle ein Ergebnis mit einem bestimmten Ursachencode generiert hat. Die Anleitungen zur Problembehebung für eine Kontrolle finden Sie in der. [Kontrollreferenz für Security Hub CSPM](#)

Ursachencode	Compliance status (Compliance-Status)	Beschreibung
CLOUDTRAIL_METRIC_FILTER_NOT_VALID	FAILED	Für den CloudTrail Trail mit mehreren Regionen gibt es keinen gültigen metrischen Filter.

Ursachencode	Compliance status (Compliance-Status)	Beschreibung
CLOUDTRAIL_METRIC_FILTERS_NOT_PRESENT	FAILED	Metrische Filter sind für den Trail mit mehreren Regionen CloudTrail nicht vorhanden.
CLOUDTRAIL_MULTI_REGION_NOT_PRESENT	FAILED	Das Konto verfügt nicht über einen CloudTrail Trail für mehrere Regionen mit der erforderlichen Konfiguration.
CLOUDTRAIL_REGION_INVALID	WARNING	CloudTrail Wanderwege mit mehreren Regionen befinden sich nicht in der aktuellen Region.
CLOUDWATCH_ALARM_ACTIONS_NOT_VALID	FAILED	Es sind keine gültigen Alarmaktionen vorhanden.
CLOUDWATCH_ALARMS_NOT_PRESENT	FAILED	CloudWatch Alarmer sind im Konto nicht vorhanden.
CONFIG_ACCESS_DENIED	NOT_AVAILABLE AWS Config Status ist ConfigError	AWS Config Zugriff verweigert. Stellen Sie sicher, dass es aktiviert AWS Config ist und dass ihm ausreichende Berechtigungen erteilt wurden.
CONFIG_EVALUATIONS_EMPTY	PASSED	AWS Config hat Ihre Ressourcen anhand der Regel bewertet. Die Regel galt nicht für die AWS Ressourcen in ihrem Geltungsbereich, die angegebenen Ressourcen wurden gelöscht oder die Bewertungsergebnisse wurden gelöscht.

Ursachencode	Compliance status (Compliance-Status)	Beschreibung
CONFIG_RECORDER_CUSTOM_ROLE	FAILED(für Config.1)	Der AWS Config Rekorder verwendet eine benutzerdefinierte IAM-Rolle anstelle der AWS Config serviceverknüpften Rolle, und der <code>includeConfigServiceLinkedRoleCheck</code> benutzerdefinierte Parameter für Config.1 ist nicht auf festgelegt. <code>false</code>
CONFIG_RECORDER_DISABLED	FAILED(für Config.1)	AWS Config ist nicht aktiviert, wenn der Konfigurationsrekorder eingeschaltet ist.
CONFIG_RECORDER_MISSING_REQUIRED_RESOURCE_TYPES	FAILED(für Config.1)	AWS Config zeichnet nicht alle Ressourcentypen auf, die den aktivierten Security Hub CSPM-Steurelementen entsprechen. Schalten Sie die Aufzeichnung für die folgenden Ressourcen ein: <i>Resources that aren't being recorded</i>

Ursachencode	Compliance status (Compliance-Status)	Beschreibung
CONFIG_RETURNS_NOT_APPLICABLE	NOT_AVAILABLE	Der Konformitätsstatus ist darauf NOT_AVAILABLE zurückzuführen, dass der Status Nicht zutreffend AWS Config zurückgegeben wurde. AWS Config gibt keinen Grund für den Status an. Hier sind einige mögliche Gründe für den Status „Nicht zutreffend“: • Die Ressource wurde aus dem Geltungsbereich der AWS Config Regel entfernt. • Die AWS Config Regel wurde gelöscht. • Die Ressource wurde gelöscht. • Die AWS Config Regellogik kann den Status Nicht zutreffend erzeugen.

Ursachencode	Compliance status (Compliance-Status)	Beschreibung
CONFIG_RULE_EVALUATION_ERROR	NOT_AVAILABLE AWS Config Der Status ist ConfigError	Dieser Ursachencode wird für verschiedene Arten von Auswertungsfehlern verwendet. Die Beschreibung enthält die spezifischen Ursacheninformationen. Die Art des Fehlers kann einer der folgenden sein: • Unmöglichkeit, die Auswertung aufgrund fehlender Berechtigungen durchzuführen. Die Beschreibung enthält die spezifische Berechtigung, die fehlt. • Ein fehlender oder ungültiger Wert für einen Parameter. Die Beschreibung enthält den Parameter und die Anforderungen für den Parameterwert. • Fehler beim Lesen aus einem S3-Bucket. Die Beschreibung identifiziert den Bucket und stellt den spezifischen Fehler bereit. • Ein fehlendes AWS Abonnement. • Ein allgemeines Timeout für die Auswertung. • Ein gesperrtes Konto.

Ursachencode	Compliance status (Compliance-Status)	Beschreibung
CONFIG_RULE_NOT_FOUND	NOT_AVAILABLE AWS Config Status ist ConfigError	Die AWS Config Regel wird gerade erstellt.
INTERNAL_SERVICE_ERROR	NOT_AVAILABLE	Es ist ein unbekannter Fehler aufgetreten.
LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE	FAILED	Security Hub CSPM kann keine Überprüfung anhand einer benutzerdefinierten Lambda-Laufzeit durchführen.
S3_BUCKET_CROSS_ACCOUNT_CROSS_REGION	WARNING	Das Ergebnis weist einen WARNING Status auf, da sich der S3-Bucket, der dieser Regel zugeordnet ist, in einer anderen Region oder einem anderen Konto befindet. Diese Regel unterstützt keine regionsübergreifenden oder kontenübergreifenden Prüfungen. Es wird empfohlen, diese Kontrolle in dieser Region oder diesem Konto zu deaktivieren. Führen Sie sie nur in der Region oder dem Konto aus, in dem sich die Ressource befindet.
SNS_SUBSCRIPTION_NOT_PRESENT	FAILED	Für die CloudWatch Logs-Metrikfilter gibt es kein gültiges Amazon SNS SNS-Abonnement.

Ursachencode	Compliance status (Compliance-Status)	Beschreibung
SNS_TOPIC_CROSS_ACCOUNT	WARNING	Das Ergebnis befindet sich in einem WARNING Zustand. Das mit dieser Regel verknüpfte SNS-Thema gehört einem anderen Konto. Das aktuelle Konto kann die Abonnementinformationen nicht abrufen. Das Konto, dem das SNS-Thema gehört, muss dem aktuellen Konto die <code>sns:ListSubscriptionsByTopic</code> Berechtigung für das SNS-Thema gewähren.
SNS_TOPIC_CROSS_ACCOUNT_CROSS_REGION	WARNING	Das Ergebnis weist einen WARNING Status auf, da sich das mit dieser Regel verknüpfte SNS-Thema in einer anderen Region oder einem anderen Konto befindet. Diese Regel unterstützt keine regionsübergreifenden oder kontenübergreifenden Prüfungen. Es wird empfohlen, diese Kontrolle in dieser Region oder diesem Konto zu deaktivieren. Führen Sie sie nur in der Region oder dem Konto aus, in dem sich die Ressource befindet.
SNS_TOPIC_INVALID	FAILED	Das mit dieser Regel verknüpfte SNS-Thema ist ungültig.

Ursachencode	Compliance status (Compliance-Status)	Beschreibung
THROTTLING_ERROR	NOT_AVAILABLE	Die entsprechende API-Operation hat die zulässige Rate überschritten.

ProductFields Einzelheiten zu den Kontrollbefunden

Bei Ergebnissen, die bei Sicherheitsprüfungen für Kontrollen generiert wurden, kann das [ProductFields](#)Attribut im AWS Security Finding Format (ASFF) die folgenden Felder enthalten.

ArchivalReasons:0/Description

Beschreibt, warum Security Hub CSPM einen Befund archiviert hat.

Security Hub CSPM archiviert beispielsweise vorhandene Ergebnisse, wenn Sie eine Kontrolle oder einen Standard deaktivieren oder wenn Sie [konsolidierte Kontrollergebnisse](#) aktivieren oder deaktivieren.

ArchivalReasons:0/ReasonCode

Gibt an, warum Security Hub CSPM einen Befund archiviert hat.

Security Hub CSPM archiviert beispielsweise vorhandene Ergebnisse, wenn Sie eine Kontrolle oder einen Standard deaktivieren oder wenn Sie [konsolidierte Kontrollergebnisse](#) aktivieren oder deaktivieren.

PreviousComplianceStatus

Der vorherige Konformitätsstatus (`Compliance.Status`) der Ressource für die angegebene Kontrolle, zum Zeitpunkt der letzten Aktualisierung des Ergebnisses. Wenn sich der Konformitätsstatus der Ressource während der letzten Aktualisierung nicht geändert hat, entspricht dieser Wert dem Wert für das `Compliance.Status` Ergebnisfeld. Eine Liste möglicher Werte finden Sie unter [Bewertung des Konformitätsstatus und des Kontrollstatus](#).

StandardsGuideArn oder StandardsArn

Der ARN des Standards, der dem Steuerelement zugeordnet ist.

Für den Benchmark-Standard der CIS AWS Foundations lautet das Feld `StandardsGuideArn`. Für die Standards PCI DSS und AWS Foundational Security Best Practices lautet das Feld `StandardsArn`.

Diese Felder werden zugunsten von `Compliance.AssociatedStandards` entfernt, wenn Sie [konsolidierte Kontrollergebnisse](#) aktivieren.

`StandardsGuideSubscriptionArn` oder `StandardsSubscriptionArn`

Der ARN des Standardabonnements des Kontos.

Für den Benchmark-Standard der CIS AWS Foundations lautet das Feld `StandardsGuideSubscriptionArn`. Für die Standards PCI DSS und AWS Foundational Security Best Practices lautet das Feld `StandardsSubscriptionArn`.

Diese Felder werden entfernt, wenn Sie [konsolidierte Kontrollergebnisse](#) aktivieren.

`RuleId` oder `ControlId`

Der Bezeichner für das Steuerelement.

Für den Benchmark-Standard der CIS AWS Foundations lautet das Feld `RuleId`. Für andere Standards ist das Feld `ControlId`.

Diese Felder werden zugunsten von `Compliance.SecurityControlId` entfernt, wenn Sie [konsolidierte Kontrollergebnisse](#) aktivieren.

`RecommendationUrl`

Die URL mit Behebungsinformationen für das Steuerelement. Dieses Feld wird entfernt, wenn Sie `Remediation.Recommendation.Url` aktivieren, wenn Sie [konsolidierte Kontrollergebnisse](#) aktivieren.

`RelatedAWSResources:0/name`

Der Name der Ressource, die dem Ergebnis zugeordnet ist.

`RelatedAWSResource:0/type`

Der Typ der Ressource, die dem Steuerelement zugeordnet ist.

`StandardsControlArn`

Der ARN des Steuerelements. Dieses Feld wird entfernt, wenn Sie [konsolidierte Kontrollergebnisse](#) aktivieren.

`aws/securityhub/ProductArn`

Für Kontrollergebnisse lautet der Produktname `Security Hub`.

aws/securityhub/CompanyName

Für Kontrollergebnisse lautet der Firmenname AWS.

aws/securityhub/annotation

Eine Beschreibung des bei der Kontrolle aufgedeckten Problems.

aws/securityhub/FindingId

Die Kennung für den Befund.

Dieses Feld verweist nicht auf einen Standard, wenn Sie [konsolidierte Kontrollergebnisse](#) aktivieren.

Schweregrade der Kontrollbefunde

Der Schweregrad, der einer Security Hub-CSPM-Steuerung zugewiesen wurde, weist auf die Wichtigkeit der Kontrolle hin. Der Schweregrad einer Kontrolle bestimmt den Schweregrad, der den Kontrollergebnissen zugewiesen wird.

Schweregradkriterien

Der Schweregrad einer Kontrolle wird anhand der folgenden Kriterien bestimmt:

- Wie schwierig ist es für einen Bedrohungsakteur, die mit der Kontrolle verbundene Konfigurationsschwäche auszunutzen? Die Schwierigkeit wird durch den Grad an Raffinesse oder Komplexität bestimmt, der erforderlich ist, um die Schwachstelle zur Ausführung eines Bedrohungsszenarios auszunutzen.
- Wie wahrscheinlich ist es, dass die Schwachstelle zu einer Beeinträchtigung Ihrer Ressourcen AWS-Konten oder Ihrer Ressourcen führt? Eine Beeinträchtigung Ihrer AWS-Konten Ressourcen bedeutet, dass die Vertraulichkeit, Integrität oder Verfügbarkeit Ihrer Daten oder AWS Infrastruktur in irgendeiner Weise beeinträchtigt wird. Die Wahrscheinlichkeit einer Gefährdung gibt an, wie wahrscheinlich es ist, dass das Bedrohungsszenario zu einer Störung oder einem Angriff auf Ihre Ressourcen AWS-Services oder Ihre Ressourcen führt.

Betrachten Sie als Beispiel die folgenden Konfigurationsschwächen:

- Benutzerzugriffsschlüssel werden nicht alle 90 Tage ausgetauscht.
- Der IAM-Root-Benutzerschlüssel ist vorhanden.

Beide Schwächen sind für einen Gegner gleichermaßen schwer auszunutzen. In beiden Fällen kann der Angreifer Anmeldeinformationen stehlen oder eine andere Methode verwenden, um an einen Benutzerschlüssel zu gelangen. Er kann es dann verwenden, um auf unautorisierte Weise auf Ihre Ressourcen zuzugreifen.

Die Wahrscheinlichkeit einer Kompromittierung ist jedoch viel höher, wenn der Bedrohungsakteur den Root-Benutzerzugriffsschlüssel erwirbt, da er dadurch besseren Zugriff hat. Infolgedessen hat die Schwäche des Root-Benutzerschlüssels einen höheren Schweregrad.

Der Schweregrad berücksichtigt nicht die Wichtigkeit der zugrunde liegenden Ressource. Kritikalität ist der Grad der Wichtigkeit der Ressourcen, die mit dem Ergebnis verknüpft sind. Beispielsweise ist eine Ressource, die einer geschäftskritischen Anwendung zugeordnet ist, kritischer als eine, die nicht produktionstechnischen Tests zugeordnet ist. Verwenden Sie das *Criticality* Feld des AWS Security Finding Formats (ASFF), um Informationen zur Ressourcenkritik zu erfassen.

In der folgenden Tabelle werden die Sicherheitsbeschriftungen aufgeführt, wie schwierig es auszunutzen ist, und wie wahrscheinlich es ist, dass sie gefährdet werden.

	Ein Kompromiss ist sehr wahrscheinlich	Kompromiss wahrscheinlich	Ein Kompromiss ist unwahrscheinlich	Ein Kompromiss ist höchst unwahrscheinlich
Sehr einfach auszunutzen	Kritisch	Kritisch	Hoch	Mittelschwer
Etwas einfach auszunutzen	Kritisch	Hoch	Mittelschwer	Mittelschwer
Etwas schwer auszunutzen	Hoch	Mittelschwer	Mittelschwer	Niedrig
Sehr schwer auszunutzen	Mittelschwer	Mittelschwer	Niedrig	Niedrig

Definitionen des Schweregrads

Die Schweregrade sind wie folgt definiert.

Kritisch — Das Problem sollte sofort behoben werden, um eine Eskalation zu vermeiden.

Beispielsweise wird ein offener S3-Bucket mit kritischem Schweregrad bewertet. Da so viele Bedrohungsakteure nach offenen S3-Buckets suchen, ist es wahrscheinlich, dass Daten in exponierten S3-Buckets von anderen entdeckt und abgerufen werden.

Im Allgemeinen gelten öffentlich zugängliche Ressourcen als kritische Sicherheitslücken. Sie sollten kritische Ergebnisse mit äußerster Dringlichkeit behandeln. Sie sollten auch die Wichtigkeit der Ressource berücksichtigen.

Hoch — Das Problem muss als kurzfristige Priorität angegangen werden.

Wenn eine Standard-VPC-Sicherheitsgruppe beispielsweise für eingehenden und ausgehenden Datenverkehr geöffnet ist, wird sie als hochgradig eingestuft. Für einen Bedrohungsakteur ist es ziemlich einfach, eine VPC mit dieser Methode zu kompromittieren. Es ist auch wahrscheinlich, dass der Bedrohungsakteur in der Lage sein wird, Ressourcen zu unterbrechen oder zu exfiltrieren, sobald sie sich in der VPC befinden.

Security Hub CSPM empfiehlt, dass Sie einen Befund mit hohem Schweregrad als kurzfristige Priorität behandeln. Sie sollten sofort Abhilfemaßnahmen ergreifen. Sie sollten auch die Wichtigkeit der Ressource berücksichtigen.

Mittel — Das Problem sollte als mittelfristige Priorität behandelt werden.

Mangelnde Verschlüsselung für Daten bei der Übertragung wird beispielsweise als mittelgradig eingestuft. Um diese Schwachstelle auszunutzen, ist ein ausgeklügelter man-in-the-middle Angriff erforderlich. Mit anderen Worten, es ist etwas schwierig. Es ist wahrscheinlich, dass einige Daten gefährdet werden, wenn das Bedrohungsszenario erfolgreich ist.

Security Hub CSPM empfiehlt, dass Sie die betroffene Ressource so schnell wie möglich untersuchen. Sie sollten auch die Wichtigkeit der Ressource berücksichtigen.

Niedrig — Das Problem erfordert keine eigenständigen Maßnahmen.

Beispielsweise wird das Versäumnis, forensische Informationen zu sammeln, als niedriger Schweregrad angesehen. Diese Kontrolle kann dazu beitragen, future Kompromisse zu verhindern, aber das Fehlen von Forensik führt nicht direkt zu einem Kompromiss.

Bei Ergebnissen mit geringem Schweregrad müssen Sie nicht sofort Maßnahmen ergreifen, aber sie können einen Kontext bieten, wenn Sie sie mit anderen Problemen korrelieren.

Informativ — Es wurde keine Sicherheitslücke in der Konfiguration gefunden.

Mit anderen Worten, der Status ist PASSEDDWARNING, oderNOT AVAILABLE.

Es gibt keine empfohlene Aktion. Informationsergebnisse helfen Kunden dabei, nachzuweisen, dass sie sich in einem konformen Zustand befinden.

Bewertung des Konformitätsstatus und des Kontrollstatus

Das `Compliance.Status` Feld des AWS Security Finding Formats beschreibt das Ergebnis eines Kontrollbefundes. AWS Security Hub Cloud Security Posture Management (CSPM) verwendet den Compliance-Status von Kontrollfeststellungen, um einen allgemeinen Kontrollstatus zu ermitteln. Der Kontrollstatus wird auf der Detailseite einer Kontrolle in der Security Hub CSPM-Konsole angezeigt.

Bewertung des Compliance-Status der CSPM-Ergebnisse von Security Hub

Dem Konformitätsstatus für jedes Ergebnis wird einer der folgenden Werte zugewiesen:

- **PASSED**— Zeigt an, dass das Steuerelement die Sicherheitsüberprüfung für den Befund bestanden hat. Dadurch wird der Security Hub CSPM `Workflow.Status` automatisch auf `eingestellt`.
RESOLVED
- **FAILED**— Zeigt an, dass das Steuerelement die Sicherheitsüberprüfung für das Ergebnis nicht bestanden hat.
- **WARNING**— Weist darauf hin, dass Security Hub CSPM nicht feststellen kann, ob sich die Ressource im Status „PASSED oder FAILED“ befindet. Beispielsweise ist die [AWS Config Ressourcenaufzeichnung](#) für den entsprechenden Ressourcentyp nicht aktiviert.
- **NOT_AVAILABLE**— Zeigt an, dass die Prüfung nicht abgeschlossen werden kann, weil ein Server ausgefallen ist, die Ressource gelöscht wurde **NOT_APPLICABLE** oder das Ergebnis der AWS Config Auswertung Wenn das AWS Config Evaluierungsergebnis war **NOT_APPLICABLE**, archiviert Security Hub CSPM den Befund automatisch.

Wenn sich der Compliance-Status für ein Ergebnis von **PASSED** zu **FAILED**, oder **WARNING** **NOT_AVAILABLE**, ändert und `Workflow.Status` entweder **NOTIFIED** oder lautet **RESOLVED**, wechselt `Workflow.Status` Security Hub CSPM automatisch zu **NEW**.

Wenn Sie nicht über Ressourcen verfügen, die einer Kontrolle entsprechen, generiert Security Hub CSPM einen **PASSED** Befund auf Kontoebene. Wenn Sie über eine Ressource verfügen, die einem Steuerelement entspricht, die Ressource dann aber löschen, erstellt Security Hub CSPM einen **NOT_AVAILABLE** Befund und archiviert ihn sofort. Nach 18 Stunden erhalten Sie einen **PASSED** Befund, da Sie nicht mehr über Ressourcen verfügen, die der Kontrolle entsprechen.

Ableitung des Kontrollstatus aus dem Compliance-Status

Security Hub CSPM leitet aus dem Compliance-Status der Kontrollfeststellungen einen allgemeinen Kontrollstatus ab. Bei der Bestimmung des Kontrollstatus ignoriert Security Hub CSPM Ergebnisse mit einem `RecordState` von `ARCHIVED` und Ergebnisse mit einem von `Workflow.Status` `SUPPRESSED`.

Dem Kontrollstatus wird einer der folgenden Werte zugewiesen:

- **Bestanden** — Zeigt an, dass alle Ergebnisse den Konformitätsstatus haben `PASSED`.
- **Fehlgeschlagen** — Zeigt an, dass mindestens ein Ergebnis den Konformitätsstatus hat `FAILED`.
- **Unbekannt** — Gibt an, dass mindestens ein Ergebnis den Konformitätsstatus `WARNING` oder `NOT_AVAILABLE` hat. Keine Ergebnisse haben den Konformitätsstatus `FAILED`.
- **Keine Daten** — Zeigt an, dass keine Ergebnisse für die Kontrolle vorliegen. Beispielsweise hat ein neu aktiviertes Steuerelement diesen Status, bis Security Hub CSPM beginnt, Ergebnisse dafür zu generieren. Ein Steuerelement hat diesen Status auch, wenn alle seine Ergebnisse aktuell nicht verfügbar sind `SUPPRESSED` oder nicht verfügbar sind. AWS-Region
- **Deaktiviert** — Zeigt an, dass das Steuerelement im aktuellen Konto und in der Region deaktiviert ist. Für dieses Steuerelement werden derzeit keine Sicherheitsüberprüfungen im Girokonto und in der Region durchgeführt. Die Ergebnisse einer deaktivierten Kontrolle können sich jedoch bis zu 24 Stunden nach der Deaktivierung auf den Compliance-Status auswirken.

Bei einem Administratorkonto spiegelt der Kontrollstatus den Kontrollstatus für das Administratorkonto und die Mitgliedskonten wider. Insbesondere wird der Gesamtstatus eines Steuerelements als Fehlgeschlagen angezeigt, wenn für das Steuerelement ein oder mehrere fehlerhafte Ergebnisse im Administratorkonto oder in einem der Mitgliedskonten gefunden wurden. Wenn Sie eine Aggregationsregion festgelegt haben, spiegelt der Kontrollstatus in der Aggregationsregion den Kontrollstatus in der Aggregationsregion und den verknüpften Regionen wider. Insbesondere wird der Gesamtstatus eines Steuerelements als Fehlgeschlagen angezeigt, wenn für das Steuerelement ein oder mehrere fehlgeschlagene Ergebnisse in der Aggregationsregion oder einer der verknüpften Regionen vorliegen.

Security Hub CSPM generiert den anfänglichen Kontrollstatus in der Regel innerhalb von 30 Minuten nach Ihrem ersten Besuch der Übersichtsseite oder der Seite Sicherheitsstandards auf der Security Hub CSPM-Konsole. Sie müssen die [AWS Config Ressourcenaufzeichnung](#) konfiguriert haben, damit der Kontrollstatus angezeigt wird. Nachdem die Kontrollstatus zum ersten Mal generiert wurden, aktualisiert Security Hub CSPM die Kontrollstatus alle 24 Stunden auf der Grundlage der Ergebnisse

der letzten 24 Stunden. Ein Zeitstempel auf der Seite mit den Kontrolldetails gibt an, wann der Kontrollstatus zuletzt aktualisiert wurde.

 Note

Nach der ersten Aktivierung eines Steuerelements kann es bis zu 24 Stunden dauern, bis Kontrollstatus in den Regionen China und den AWS GovCloud (US) Region generiert werden.

Berechnung von Sicherheitswerten

Auf der AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole werden auf der Übersichtsseite und der Kontrollseite eine Zusammenfassung der Sicherheitsbewertung für alle Ihre aktivierten Standards angezeigt. Auf der Seite Sicherheitsstandards zeigt Security Hub CSPM außerdem eine Sicherheitsbewertung von 0 bis 100 Prozent für jeden aktivierten Standard an.

Wenn Sie Security Hub CSPM zum ersten Mal aktivieren, berechnet Security Hub CSPM die zusammenfassende Sicherheitsbewertung und die Standardsicherheitsbewertungen innerhalb von 30 Minuten nach Ihrem ersten Besuch der Seite Zusammenfassung oder Sicherheitsstandards auf der Konsole. Bewertungen werden nur für Standards generiert, die aktiviert sind, wenn Sie diese Seiten auf der Konsole aufrufen. Darüber hinaus muss die AWS Config Ressourcenaufzeichnung konfiguriert werden, damit die Ergebnisse angezeigt werden. Die zusammenfassende Sicherheitsbewertung ist der Durchschnitt der Standardsicherheitsbewertungen. Um eine Liste der derzeit aktivierten Standards zu überprüfen, können Sie den [GetEnabledStandards](#) Betrieb der Security Hub CSPM-API verwenden.

Nach der erstmaligen Score-Generierung aktualisiert Security Hub CSPM die Sicherheitswerte alle 24 Stunden. Security Hub CSPM zeigt einen Zeitstempel an, der angibt, wann eine Sicherheitsbewertung zuletzt aktualisiert wurde. Beachten Sie, dass es bis zu 24 Stunden dauern kann, bis zum ersten Mal Sicherheitsbewertungen in den China Regionen und AWS GovCloud (US) Regions generiert werden.

Wenn Sie die Option „[Konsolidierte Kontrollergebnisse](#)“ aktivieren, kann es bis zu 24 Stunden dauern, bis Ihre Sicherheitsbewertungen aktualisiert werden. Darüber hinaus werden durch die Aktivierung einer neuen Aggregationsregion oder die Aktualisierung verknüpfter Regionen bestehende Sicherheitsbewertungen zurückgesetzt. Es kann bis zu 24 Stunden dauern, bis Security Hub CSPM neue Sicherheitsbewertungen generiert, die Daten aus den aktualisierten Regionen enthalten.

Methode zur Berechnung von Sicherheitswerten

Sicherheitswerte stellen das Verhältnis zwischen bestandenen Kontrollen und aktivierten Kontrollen dar. Die Punktzahl wird als Prozentsatz angezeigt, auf die nächste ganze Zahl auf- oder abgerundet.

Security Hub CSPM berechnet eine zusammenfassende Sicherheitsbewertung für alle Ihre aktivierten Standards. Security Hub CSPM berechnet außerdem eine Sicherheitsbewertung für jeden aktivierten Standard. Für die Berechnung der Punktzahl umfassen aktivierte Kontrollen Kontrollen mit dem Status „Bestanden“, „Fehlgeschlagen“ und „Unbekannt“. Steuerelemente mit dem Status Keine Daten sind von der Punkteberechnung ausgeschlossen.

Security Hub CSPM ignoriert archivierte und unterdrückte Ergebnisse bei der Berechnung des Kontrollstatus. Dies kann sich auf die Sicherheitswerte auswirken. Wenn Sie beispielsweise alle fehlgeschlagenen Ergebnisse für eine Kontrolle unterdrücken, erhält sie den Status Bestanden, was wiederum Ihre Sicherheitswerte verbessern kann. Weitere Informationen zum Kontrollstatus finden Sie unter [Bewertung des Konformitätsstatus und des Kontrollstatus](#).

Beispiel für eine Bewertung:

Standard	Kontrollen bestanden	Fehlgeschlagene Kontrollen	Unbekannte Kontrollen	Standardp unktzahl
AWS Bewährte grundlege nde Sicherhei tsmethoden v1.0.0	168	22	0	88%
Benchmark AWS v1.4.0 für GUS- Stiftungen	8	29	0	22%
Benchmark AWS v1.2.0 für GUS- Stiftungen	6	35	0	15%
NIST-Sond erpublikation	159	56	0	74%

Standard	Kontrollen bestanden	Fehlgeschlagene Kontrollen	Unbekannte Kontrollen	Standardp unktzahl
800-53 Revision 5				
PCI DSS v3.2.1	28	17	0	62%

Bei der Berechnung der zusammenfassenden Sicherheitsbewertung zählt Security Hub CSPM jede Kontrolle standardübergreifend nur einmal. Wenn Sie beispielsweise ein Steuerelement aktiviert haben, das für drei aktivierte Standards gilt, zählt es für Bewertungszwecke nur als ein aktiviertes Steuerelement.

In diesem Beispiel beträgt die Gesamtzahl der aktivierten Kontrollen für alle aktivierten Standards zwar 528, Security Hub CSPM zählt jedoch jedes einzelne Steuerelement zu Bewertungszwecken nur einmal. Die Anzahl der einzelnen aktivierten Kontrollen liegt wahrscheinlich unter 528. Wenn wir davon ausgehen, dass die Anzahl der eindeutigen aktivierten Kontrollen 515 und die Anzahl der eindeutigen bestandenen Kontrollen 357 beträgt, liegt der Gesamtwert bei 69%. Diese Punktzahl wird berechnet, indem die Anzahl der eindeutigen bestandenen Kontrollen durch die Anzahl der eindeutigen aktivierten Kontrollen dividiert wird.

Möglicherweise haben Sie eine Gesamtpunktzahl, die von der Standardsicherheitsbewertung abweicht, auch wenn Sie in Ihrem Konto in der aktuellen Region nur einen Standard aktiviert haben. Dies kann der Fall sein, wenn Sie mit einem Administratorkonto angemeldet sind und für Mitgliedskonten zusätzliche Standards oder andere Standards aktiviert sind. Dies kann auch der Fall sein, wenn Sie sich die Punktzahl aus der Aggregationsregion ansehen und zusätzliche Standards oder andere Standards in verknüpften Regionen aktiviert sind.

Sicherheitsbewertungen für Administratorkonten

Wenn Sie mit einem Administratorkonto angemeldet sind, beziehen sich die Sicherheitsbewertung und die Standardwerte auf den Kontrollstatus im Administratorkonto und in allen Mitgliedskonten.

Wenn der Status einer Kontrolle auch nur in einem Mitgliedskonto Fehlgeschlagen lautet, lautet ihr Status im Administratorkonto Fehlgeschlagen und wirkt sich auf die Punktzahlen des Administratorkontos aus.

Wenn Sie mit einem Administratorkonto angemeldet sind und Ergebnisse in einer Aggregationsregion anzeigen, berücksichtigen die Sicherheitsbewertungen den Kontrollstatus in allen Mitgliedskonten und allen verknüpften Regionen.

Sicherheitswerte, wenn Sie eine Aggregationsregion festgelegt haben

Wenn Sie eine Aggregation festgelegt haben AWS-Region, berücksichtigen die zusammenfassende Sicherheitsbewertung und die Standardwerte den Kontrollstatus in allen Bereichen verknüpfte Regionen.

Wenn der Status eines Steuerelements auch nur in einer verknüpften Region Fehlgeschlagen lautet, lautet sein Status in der Aggregationsregion Fehlgeschlagen, was sich auf die Werte der Aggregationsregion auswirkt.

Wenn Sie mit einem Administratorkonto angemeldet sind und sich Punktzahlen in einer Aggregationsregion ansehen, berücksichtigen die Sicherheitsbewertungen den Kontrollstatus in allen Mitgliedskonten und allen verknüpften Regionen.

Kontrollkategorien in Security Hub CSPM

Jedem Steuerelement wird eine Kategorie zugewiesen. Die Kategorie einer Kontrolle spiegelt die Sicherheitsfunktion wider, auf die die Kontrolle angewendet wird.

Der Kategoriewert enthält die Kategorie, die Unterkategorie innerhalb der Kategorie und optional einen Klassifikator innerhalb der Unterkategorie. Zum Beispiel:

- Identifizieren > Inventar
- Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Hier finden Sie die Beschreibungen der verfügbaren Kategorien, Unterkategorien und Klassifikatoren.

Identifizieren

Entwickeln Sie die organisatorische Grundlagen für das Management von Cybersicherheitsrisiken für Systeme, Assets, Daten und Funktionen.

Bestand

Hat der Service die richtigen Ressourcen-Tagging-Strategien implementiert? Schließen die Tagging-Strategien den Ressourcenbesitzer ein?

Welche Ressourcen werden vom Service genutzt? Sind sie für diesen Service genehmigte Ressourcen?

Haben Sie Einblick in den genehmigten Bestand? Verwenden Sie beispielsweise Dienste wie Amazon EC2 Systems Manager und Service Catalog?

Protokollierung

Haben Sie die gesamte relevante Protokollierung für den Service sicher aktiviert? Beispiele für Protokolldateien sind die folgenden:

- Amazon VPC-Flussprotokolle
- Zugriffsprotokolle für Elastic Load Balancing
- CloudFront Amazon-Protokolle
- CloudWatch Amazon-Protokolle
- Protokollierung durch Amazon Relational Database Service
- Langsame Indexprotokolle von Amazon OpenSearch Service
- X-Ray-Nachverfolgung
- AWS Directory Service Protokolle
- AWS Config Artikel
- Snapshots

Schutz

Entwicklung und Implementierung geeigneter Sicherheitsvorkehrungen, um die Bereitstellung kritischer Infrastrukturservices und sicherer Codierungspraktiken zu gewährleisten.

Sichere Zugriffsverwaltung

Verwendet der Service in seinen IAM- oder Ressourcenrichtlinien Verfahren mit den geringsten Rechten?

Sind Passwörter und Secrets ausreichend komplex? Werden sie angemessen rotiert?

Verwendet der Service Multi-Factor Authentication (MFA)?

Vermeidet der Dienst den Root-Benutzer?

Erlauben ressourcenbasierte Richtlinien den öffentlichen Zugriff?

Sichere Netzwerkkonfiguration

Vermeidet der Service öffentlichen und unsicheren Remote-Netzwerkzugriff?

Wird der Dienst VPCs ordnungsgemäß verwendet? Müssen beispielsweise Jobs ausgeführt werden VPCs?

Segmentiert und isoliert der Service sensible Ressourcen ordnungsgemäß?

Datenschutz

Verschlüsselung von Daten im Ruhezustand — Verschlüsselt der Dienst Daten im Ruhezustand?

Verschlüsselung von Daten bei der Übertragung — Verschlüsselt der Dienst Daten bei der Übertragung?

Datenintegrität — Validiert der Dienst Daten auf Integrität?

Schutz vor Datenlöschung — Schützt der Dienst Daten vor versehentlichem Löschen?

Datenverwaltung/-nutzung — Verwenden Sie Dienste wie Amazon Macie, um den Standort Ihrer sensiblen Daten zu verfolgen?

API-Schutz

Wird der Service AWS PrivateLink zum Schutz der Service-API-Operationen verwendet?

Schutzdienste

Sind die richtigen Schutzdienste vorhanden? Bieten sie das richtige Maß an Abdeckung?

Schutzdienste helfen Ihnen, Angriffe und Gefährdungen abzuwehren, die auf den Service abzielen. Beispiele für Schutzdienste AWS sind AWS Control Tower, AWS WAF, Vanta AWS Shield Advanced, Secrets Manager, IAM Access Analyzer und AWS Resource Access Manager

Sichere Entwicklung

Verwenden Sie sichere Codierungspraktiken?

Vermeiden Sie Schwachstellen wie das Open Web Application Security Project (OWASP) Top Ten?

Detect

Entwickeln und implementieren Sie geeignete Aktivitäten, um das Auftreten eines Cybersicherheitsereignisses zu identifizieren.

Erkennungsservices

Sind die richtigen Erkennungsservices vorhanden?

Bieten sie das richtige Maß an Abdeckung?

Zu den AWS Erkennungsdiensten gehören Amazon GuardDuty, AWS Security Hub Cloud Security Posture Management (CSPM), Amazon Inspector, Amazon Detective, Amazon CloudWatch Alarms und AWS IoT Device Defender. AWS Trusted Advisor

Reagieren

Entwickeln und implementieren Sie geeignete Aktivitäten, um Maßnahmen in Bezug auf ein erkanntes Cybersicherheitsereignis zu ergreifen.

Reaktionsaktionen

Reagieren Sie schnell auf Sicherheitsereignisse?

Verfügen Sie über aktive Ergebnisse mit kritischem oder hohem Schweregrad?

Forensik

Können Sie sicher forensische Daten für den Service erfassen? Erwerben Sie beispielsweise Amazon EBS-Snapshots, die mit wirklich positiven Ergebnissen verknüpft sind?

Haben Sie ein forensisches Konto eingerichtet?

Wiederherstellung

Entwickeln und implementieren Sie geeignete Aktivitäten, um Ausfallpläne aufrechtzuerhalten und alle Funktionen oder Services wiederherzustellen, die aufgrund eines Cybersicherheitsereignisses beeinträchtigt wurden.

Ausfallsicherheit

Unterstützt die Servicekonfiguration ordnungsgemäße Failovers, elastische Skalierung und hohe Verfügbarkeit?

Haben Sie Sicherungen erstellt?

Überprüfung der Details der Kontrollen in Security Hub CSPM

Wenn Sie auf der Kontrollseite oder der Standarddetailseite der Security Hub CSPM-Konsole ein Steuerelement auswählen, gelangen Sie zu einer Seite mit Kontrolldetails.

Oben auf der Seite mit den Kontrolldetails wird der Kontrollstatus angezeigt. Der Kontrollstatus fasst die Leistung einer Kontrolle auf der Grundlage des Konformitätsstatus der Kontrollergebnisse zusammen. Security Hub CSPM generiert den anfänglichen Kontrollstatus in der Regel innerhalb von 30 Minuten nach Ihrem ersten Besuch der Übersichtsseite oder der Seite Sicherheitsstandards auf der Security Hub CSPM-Konsole. Status sind nur für Kontrollen verfügbar, die aktiviert werden, wenn Sie diese Seiten besuchen.

Auf der Seite mit den Kontrolldetails finden Sie auch eine Aufschlüsselung des Konformitätsstatus der Kontrollergebnisse der letzten 24 Stunden. Weitere Informationen zum Kontrollstatus und zum Compliance-Status finden Sie unter [Bewertung des Konformitätsstatus und des Kontrollstatus](#).

AWS Config Die Ressourcenaufzeichnung muss konfiguriert sein, damit der Kontrollstatus angezeigt wird. Nachdem der Kontrollstatus zum ersten Mal generiert wurde, aktualisiert Security Hub CSPM den Kontrollstatus alle 24 Stunden auf der Grundlage der Ergebnisse der letzten 24 Stunden.

Für Administratorkonten wird ein aggregierter Kontrollstatus für das Administratorkonto und die Mitgliedskonten angezeigt. Wenn Sie eine Aggregationsregion festgelegt haben, umfasst der Kontrollstatus Ergebnisse aus allen verknüpften Regionen. Weitere Informationen zum Kontrollstatus finden Sie unter [the section called “Konformitätsstatus und Kontrollstatus”](#).

Sie können die Steuerung auch auf der Seite mit den Kontrolldetails aktivieren oder deaktivieren.

Note

Nach der Aktivierung eines Steuerelements kann es bis zu 24 Stunden dauern, bis in den Regionen China und erstmalige Kontrollstatus generiert werden. AWS GovCloud (US) Regions

Auf der Registerkarte „Standards und Anforderungen“ sind die Standards aufgeführt, für die eine Kontrolle aktiviert werden kann, sowie die Anforderungen, die sich aus den verschiedenen Compliance-Frameworks ergeben, in Bezug auf die Kontrolle.

Auf der Registerkarte „Prüfungen“ werden die für die Kontrolle aktiven Ergebnisse der letzten 24 Stunden aufgeführt. Kontrollergebnisse werden generiert und aktualisiert, wenn Security Hub CSPM

Sicherheitsprüfungen für die Kontrolle durchführt. Die Liste auf dieser Registerkarte enthält keine archivierten Ergebnisse.

Für jedes Ergebnis bietet die Liste Zugriff auf Ergebnisdetails wie den Konformitätsstatus und die zugehörige Ressource. Sie können auch den Workflow-Status für jedes Ergebnis festlegen und Ergebnisse an benutzerdefinierte Aktionen senden. Weitere Informationen finden Sie unter [Überprüfung und Verwaltung der Kontrollergebnisse](#).

Details für ein Steuerelement anzeigen

Wählen Sie Ihre bevorzugte Zugriffsmethode und gehen Sie wie folgt vor, um die Details für ein Steuerelement zu überprüfen. Die Angaben beziehen sich auf das Girokonto und die Region und beinhalten Folgendes:

- Der Titel und die Beschreibung der Kontrolle.
- Ein Link zu Anleitungen zur Behebung fehlgeschlagener Kontrollergebnisse.
- Der Schweregrad der Kontrolle.
- Der Status der Kontrolle.

Auf der Konsole können Sie sich auch eine Liste der aktuellen Ergebnisse der Kontrolle ansehen. Um dies programmgesteuert zu tun, können Sie den [GetFindings](#) Betrieb der Security Hub CSPM-API verwenden.

Security Hub CSPM console

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Controls aus.
3. Wählen Sie ein Steuerelement aus.

Security Hub CSPM API

1. Führen Sie [ListSecurityControlDefinitions](#) einen oder mehrere Standards aus und geben Sie ARNs sie an, um eine Liste der Steuerelemente IDs für diesen Standard zu erhalten. Um den Standard zu erhalten ARNs, führen Sie den Befehl aus [DescribeStandards](#). Wenn Sie keinen Standard-ARN angeben, gibt diese API die gesamte Security Hub CSPM-Steuerung zurück. IDs Diese API gibt eine

standardunabhängige Sicherheitskontrolle zurück IDs, nicht die standardbasierte Steuerung IDs , die vor diesen Feature-Releases existierte.

Beispiel für eine Anfrage:

```
{
  "StandardsArn": "arn:aws:securityhub::standards/aws-foundational-security-best-practices/v/1.0.0"
}
```

2. Ausführen [BatchGetSecurityControls](#), um Details zu einem oder mehreren Steuerelementen im aktuellen AWS-Konto und abzurufen AWS-Region.

Beispiel für eine Anfrage:

```
{
  "SecurityControlIds": ["Config.1", "IAM.1"]
}
```

AWS CLI

1. Führen Sie den [list-security-control-definitions](#) Befehl aus und geben Sie einen oder mehrere Standards ARNs an, um eine Liste von Steuerelementen zu erhalten IDs. Führen Sie den describe-standards Befehl aus ARNs, um den Standard zu erhalten. Wenn Sie keinen Standard-ARN angeben, gibt dieser Befehl die gesamte Security Hub-CSPM-Steuerung zurück. IDs Dieser Befehl gibt eine standardunabhängige Sicherheitskontrolle zurück IDs, nicht die standardbasierte Steuerung IDs , die vor diesen Feature-Releases existierte.

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0"
```

2. Führen Sie den [batch-get-security-controls](#) Befehl aus, um Details zu einem oder mehreren Steuerelementen im aktuellen und abzurufen. AWS-Konto AWS-Region

```
aws securityhub --region us-east-1 batch-get-security-controls --security-
control-ids '["Config.1", "IAM.1"]'
```

Filter- und Sortiersteuerungen in Security Hub CSPM

Auf der AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole können Sie auf der Seite „Kontrollen“ eine Tabelle mit den derzeit verfügbaren Kontrollen überprüfen. AWS-Region Die Ausnahme ist eine Aggregationsregion. Wenn Sie [eine Aggregationsregion konfiguriert](#) haben und sich bei dieser Region anmelden, werden in der Konsole Steuerelemente angezeigt, die in der Aggregationsregion oder einer oder mehreren verknüpften Regionen verfügbar sind.

Um sich auf eine bestimmte Teilmenge von Steuerelementen zu konzentrieren, können Sie die Tabelle der Steuerelemente sortieren und filtern. Mithilfe der Optionen „Nach filtern“ neben der Tabelle können Sie sich schnell auf diese bestimmten Teilmengen konzentrieren:

- Alle aktivierten Steuerelemente, d. h. Steuerelemente, die in mindestens einem aktivierten Standard aktiviert sind.
- Alle deaktivierten Steuerelemente, d. h. Steuerelemente, die in allen Standards deaktiviert sind.
- Alle aktivierten Steuerelemente, die einen bestimmten Steuerstatus haben, z. B. Fehlgeschlagen. Mit der Option Keine Daten werden nur die Steuerelemente angezeigt, für die derzeit keine Ergebnisse vorliegen. Informationen zum Kontrollstatus finden Sie unter [Bewertung des Konformitätsstatus und des Kontrollstatus](#).

Zusätzlich zu den Optionen Nach filtern können Sie die Tabelle filtern, indem Sie Filterkriterien in das Feld Steuerelemente filtern über der Tabelle eingeben. Sie können beispielsweise nach Kontroll-ID oder Schweregrad filtern.

Standardmäßig werden Steuerelemente mit dem Status Fehlgeschlagen zuerst aufgeführt, in absteigender Reihenfolge nach Schweregrad. Sie können die Sortierreihenfolge ändern, indem Sie eine andere Spaltenüberschrift auswählen.

Tip

Wenn Sie automatisierte Workflows haben, die auf Kontrollergebnissen basieren, empfehlen wir, die [Felder SecurityControlId oder SecurityControlArn ASFF](#) als Filter zu verwenden, anstatt die Description Felder Title oder. Letztere Felder können sich gelegentlich ändern, wohingegen Kontroll-ID und ARN statische Identifikatoren sind.

Wenn Sie mit einem Security Hub CSPM-Administratorkonto angemeldet sind, gehören zu den aktivierten Steuerelementen auch Steuerelemente, die in mindestens einem Mitgliedskonto

aktiviert sind. Wenn Sie eine Aggregationsregion konfiguriert haben, gehören zu den aktivierten Steuerelementen auch Steuerelemente, die in mindestens einer verknüpften Region aktiviert sind.

Wenn Sie die Option neben einem aktivierten Steuerelement auswählen, wird ein Fenster mit den Standards angezeigt, in denen das Steuerelement derzeit aktiviert ist. Sie können auch die Standards sehen, in denen das Steuerelement derzeit deaktiviert ist. In diesem Bereich können Sie ein Steuerelement in allen Standards deaktivieren. Weitere Informationen finden Sie unter [Steuerelemente in Security Hub CSPM deaktivieren](#). Bei Administratorkonten spiegeln die Informationen im Panel die Einstellungen für all Ihre Mitgliedskonten wider.

Um eine Liste von Steuerelementen programmgesteuert abzurufen, können Sie den [ListSecurityControlDefinitions](#) Betrieb der Security Hub CSPM-API verwenden. Verwenden Sie den Vorgang, um die Details einzelner Steuerelemente abzurufen. [BatchGetSecurityControls](#)

Grundlegendes zu den Steuerparametern in Security Hub CSPM

Einige Kontrollen in AWS Security Hub Cloud Security Posture Management (CSPM) verwenden Parameter, die beeinflussen, wie die Kontrolle bewertet wird. In der Regel werden solche Kontrollen anhand der von Security Hub CSPM definierten Standardparameterwerte bewertet. Für eine Teilmenge dieser Steuerelemente können Sie die Parameterwerte jedoch ändern. Wenn Sie einen Steuerparameterwert ändern, beginnt Security Hub CSPM, die Steuerung anhand des von Ihnen angegebenen Werts auszuwerten. Wenn die dem Steuerelement zugrunde liegende Ressource den benutzerdefinierten Wert erfüllt, generiert Security Hub CSPM einen Befund. PASSED Wenn die Ressource den benutzerdefinierten Wert nicht erfüllt, generiert Security Hub CSPM einen FAILED Befund.

Durch die Anpassung der Kontrollparameter können Sie die von Security Hub CSPM empfohlenen und überwachten bewährten Sicherheitsmethoden verfeinern, um sie an Ihre Geschäftsanforderungen und Sicherheitserwartungen anzupassen. Anstatt die Ergebnisse einer Kontrolle zu unterdrücken, können Sie einen oder mehrere ihrer Parameter anpassen, um Ergebnisse zu erhalten, die Ihren Sicherheitsanforderungen entsprechen.

Im Folgenden finden Sie einige Anwendungsbeispiele für das Ändern von Steuerparametern und das Festlegen benutzerdefinierter Werte:

- [CloudWatch.16] — CloudWatch Protokollgruppen sollten für einen bestimmten Zeitraum aufbewahrt werden

Sie können den Aufbewahrungszeitraum angeben.

- [IAM.7] — Passwortrichtlinien für IAM-Benutzer sollten solide Konfigurationen haben

Sie können Parameter für die Passwortstärke angeben.

- [EC2.18] — Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Verkehr für autorisierte Ports zulassen

Sie können angeben, welche Ports uneingeschränkten eingehenden Verkehr zulassen dürfen.

- [Lambda.5] — VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren

Sie können die Mindestanzahl von Availability Zones angeben, die zu einem erfolgreichen Ergebnis führen.

In diesem Abschnitt werden Dinge behandelt, die Sie bei der Änderung von Steuerungsparametern beachten sollten.

Auswirkung der Änderung von Steuerparameterwerten

Wenn Sie einen Parameterwert ändern, lösen Sie auch eine neue Sicherheitsüberprüfung aus, bei der das Steuerelement anhand des neuen Werts bewertet wird. Security Hub CSPM generiert dann neue Kontrollergebnisse auf der Grundlage des neuen Werts. Bei regelmäßigen Updates zur Kontrolle der Ergebnisse verwendet Security Hub CSPM auch den neuen Parameterwert. Wenn Sie Parameterwerte für ein Steuerelement ändern, aber keine Standards aktiviert haben, die das Steuerelement enthalten, führt Security Hub CSPM keine Sicherheitsprüfungen mit den neuen Werten durch. Sie müssen mindestens einen relevanten Standard für Security Hub CSPM aktivieren, um die Kontrolle auf der Grundlage des neuen Parameterwerts auszuwerten.

Ein Steuerelement kann einen oder mehrere anpassbare Parameter haben. Zu den möglichen Datentypen für jeden Steuerparameter gehören die folgenden:

- Boolesch
- Double
- Enum
- EnumList
- Ganzzahl
- IntegerList
- String

- StringList

Benutzerdefinierte Parameterwerte gelten für alle Ihre aktivierten Standards. Sie können die Parameter für ein Steuerelement, das in Ihrer aktuellen Region nicht unterstützt wird, nicht anpassen. Eine Liste der regionalen Grenzwerte für einzelne Steuerelemente finden Sie unter [Regionale Beschränkungen der Security Hub CSPM-Steuerungen](#).

Bei einigen Kontrollen müssen akzeptable Parameterwerte in einen bestimmten Bereich fallen, um gültig zu sein. In diesen Fällen bietet Security Hub CSPM den akzeptablen Bereich.

Security Hub CSPM wählt Standardparameterwerte und aktualisiert sie möglicherweise gelegentlich. Nachdem Sie einen Steuerparameter angepasst haben, entspricht sein Wert weiterhin dem Wert, den Sie für den Parameter angegeben haben, sofern Sie ihn nicht ändern. Das heißt, der Parameter stoppt die Nachverfolgung von Aktualisierungen des Security Hub CSPM-Standardwerts, auch wenn der benutzerdefinierte Wert des Parameters mit dem aktuellen, von Security Hub CSPM definierten Standardwert übereinstimmt. Hier ist ein Beispiel für die Steuerung [ACM.1] — Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden:

```
{
  "SecurityControlId": "ACM.1",
  "Parameters": {
    "daysToExpiration": {
      "ValueType": "CUSTOM",
      "Value": {
        "Integer": 30
      }
    }
  }
}
```

Im vorherigen Beispiel hat der `daysToExpiration` Parameter den benutzerdefinierten Wert. 30 Der aktuelle Standardwert für diesen Parameter ist ebenfalls 30. Wenn Security Hub CSPM den Standardwert auf 14 ändert, verfolgt der Parameter in diesem Beispiel diese Änderung nicht. Er behält den Wert von. 30

Wenn Sie Aktualisierungen des Security Hub CSPM-Standardwerts für einen Parameter verfolgen möchten, setzen Sie das `ValueType` Feld auf `DEFAULT` statt auf `CUSTOM`. Weitere Informationen finden Sie unter [Zurücksetzen auf die Standardsteuerungsparameter in einem einzigen Konto und einer Region](#).

Steuerelemente, die benutzerdefinierte Parameter unterstützen

Eine Liste der Sicherheitskontrollen, die benutzerdefinierte Parameter unterstützen, finden Sie auf der Seite Kontrollen der Security Hub CSPM-Konsole oder unter [Kontrollreferenz für Security Hub CSPM](#). Um diese Liste programmgesteuert abzurufen, können Sie den Vorgang verwenden [ListSecurityControlDefinitions](#). In der Antwort gibt das CustomizableProperties Objekt an, welche Steuerelemente anpassbare Parameter unterstützen.

Überprüfung der aktuellen Steuerparameterwerte

Es kann hilfreich sein, den aktuellen Wert eines Steuerparameters zu kennen, bevor Sie ihn ändern.

Sie können die aktuellen Werte für einzelne Steuerparameter in Ihrem Konto überprüfen. Wenn Sie die zentrale Konfiguration verwenden, kann der delegierte AWS Security Hub Cloud Security Posture Management (CSPM) -Administrator auch Parameterwerte überprüfen, die in einer Konfigurationsrichtlinie angegeben sind.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um die aktuellen Kontrollparameterwerte zu überprüfen.

Security Hub CSPM console

Um die aktuellen Steuerparameterwerte zu überprüfen (Konsole)

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Controls aus. Wählen Sie ein Steuerelement aus.
3. Wählen Sie die Registerkarte Parameters aus. Auf dieser Registerkarte werden die aktuellen Parameterwerte für das Steuerelement angezeigt.

Security Hub CSPM API

Um die aktuellen Steuerparameterwerte (API) zu überprüfen

Rufen Sie die [BatchGetSecurityControls](#) API auf und stellen Sie eine oder mehrere Sicherheitskontrollen bereit IDs oder ARNs. Das Parameters Objekt in der Antwort zeigt die aktuellen Parameterwerte für die angegebenen Steuerelemente an.

Der folgende AWS CLI Befehl zeigt beispielsweise die aktuellen Parameterwerte für `APIGateway.1`, `CloudWatch.15`, und `IAM.7`. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (`\`) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub batch-get-security-controls \  
--region us-east-1 \  
--security-control-ids '["APIGateway.1", "CloudWatch.15", "IAM.7"]'
```

Wählen Sie Ihre bevorzugte Methode, um die aktuellen Parameterwerte in einer zentralen Konfigurationsrichtlinie anzuzeigen.

Security Hub CSPM console

Um die aktuellen Kontrollparameterwerte in einer Konfigurationsrichtlinie (Konsole) zu überprüfen

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>

Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub CSPM-Administratorkontos in der Heimatregion an.

2. Wählen Sie im Navigationsbereich Einstellungen und Konfiguration aus.
3. Wählen Sie auf der Registerkarte Richtlinien die Konfigurationsrichtlinie aus und klicken Sie dann auf Details anzeigen. Anschließend werden die Richtliniendetails angezeigt, einschließlich der aktuellen Parameterwerte.

Security Hub CSPM API

Um die aktuellen Steuerparameterwerte in einer Konfigurationsrichtlinie (API) zu überprüfen

1. Rufen Sie die [GetConfigurationPolicy](#) API über das delegierte Administratorkonto in der Heimatregion auf.
2. Geben Sie den ARN oder die ID der Konfigurationsrichtlinie an, deren Details Sie sehen möchten. Die Antwort enthält aktuelle Parameterwerte.

Mit dem folgenden AWS CLI Befehl werden beispielsweise die aktuellen Steuerparameterwerte in der angegebenen Konfigurationsrichtlinie abgerufen. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub get-configuration-policy \
--region us-east-1 \
--identifizier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Zu den Kontrollergebnissen gehören auch die aktuellen Werte der Steuerparameter. In der [AWS Format für Sicherheitssuche \(ASFF\)](#) erscheinen diese Werte im Parameters Feld des Compliance Objekts. Um die Ergebnisse auf der Security Hub CSPM-Konsole zu überprüfen, wählen Sie im Navigationsbereich Findings aus. Verwenden Sie den [GetFindings](#) Betrieb der Security Hub CSPM-API, um die Ergebnisse programmatisch zu überprüfen.

Anpassen von Steuerparameterwerten

Die Anweisungen zum Anpassen der Steuerparameter variieren je nachdem, ob Sie die [zentrale Konfiguration](#) in AWS Security Hub Cloud Security Posture Management (CSPM) verwenden. Die zentrale Konfiguration ist eine Funktion, mit der der delegierte Security Hub CSPM-Administrator die Security Hub CSPM-Funktionen für Konten und Organisationseinheiten AWS-Regionen konfigurieren kann (). OUs

Wenn Ihr Unternehmen die zentrale Konfiguration verwendet, kann der delegierte Administrator Konfigurationsrichtlinien erstellen, die benutzerdefinierte Steuerungsparameter enthalten. Diese Richtlinien können mit zentral verwalteten Mitgliedskonten verknüpft werden und OUs treten in Ihrer Heimatregion und allen verknüpften Regionen in Kraft. Der delegierte Administrator kann auch ein oder mehrere Konten als selbstverwaltete Konten festlegen, sodass der Kontoinhaber seine eigenen Parameter in jeder Region separat konfigurieren kann. Wenn Ihre Organisation keine zentrale Konfiguration verwendet, müssen Sie die Steuerparameter für jedes Konto und jede Region separat anpassen.

Wir empfehlen, die zentrale Konfiguration zu verwenden, da Sie so die Werte der Steuerparameter in verschiedenen Teilen Ihrer Organisation aufeinander abstimmen können. Beispielsweise könnten alle Ihre Testkonten bestimmte Parameterwerte verwenden, und alle Produktionskonten könnten unterschiedliche Werte verwenden.

Anpassen der Steuerparameter in mehreren Konten und Regionen

Wenn Sie der delegierte Security Hub CSPM-Administrator für eine Organisation sind, die die zentrale Konfiguration verwendet, wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um die Steuerungsparameter für mehrere Konten und Regionen anzupassen.

Security Hub CSPM console

So passen Sie die Werte der Steuerparameter in mehreren Konten und Regionen an (Konsole)

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>

Stellen Sie sicher, dass Sie in der Heimatregion angemeldet sind.

2. Wählen Sie im Navigationsbereich Einstellungen und Konfiguration aus.
3. Wählen Sie die Registerkarte Policies.
4. Um eine neue Konfigurationsrichtlinie mit benutzerdefinierten Parametern zu erstellen, wählen Sie Richtlinie erstellen aus. Um benutzerdefinierte Parameter in einer vorhandenen Konfigurationsrichtlinie anzugeben, wählen Sie die Richtlinie aus und klicken Sie dann auf Bearbeiten.

Um eine neue Konfigurationsrichtlinie mit benutzerdefinierten Steuerparameterwerten zu erstellen

1. Wählen Sie im Abschnitt Benutzerdefinierte Richtlinie die Sicherheitsstandards und Kontrollen aus, die Sie aktivieren möchten.
2. Wählen Sie Steuerungsparameter anpassen aus.
3. Wählen Sie ein Steuerelement aus, und geben Sie dann benutzerdefinierte Werte für einen oder mehrere Parameter an.
4. Um Parameter für weitere Steuerelemente anzupassen, wählen Sie Zusätzliche Steuerung anpassen.
5. Wählen Sie im Abschnitt Konten die Konten aus OUs , auf die Sie die Richtlinie anwenden möchten.
6. Wählen Sie Weiter aus.
7. Wählen Sie Richtlinie erstellen und anwenden. In Ihrer Heimatregion und allen verknüpften Regionen setzt diese Aktion die vorhandenen Konfigurationseinstellungen der Konten außer Kraft OUs , die mit dieser Konfigurationsrichtlinie verknüpft sind. Konten und

OUs können durch direkte Anwendung oder Vererbung von einem Elternteil mit einer Konfigurationsrichtlinie verknüpft werden.

Um die Werte der Steuerparameter in einer vorhandenen Konfigurationsrichtlinie anzupassen

1. Geben Sie im Abschnitt Steuerelemente unter Benutzerdefinierte Richtlinie die gewünschten neuen benutzerdefinierten Parameterwerte an.
2. Wenn Sie in dieser Richtlinie zum ersten Mal Steuerparameter anpassen, wählen Sie Steuerparameter anpassen aus und wählen Sie dann ein Steuerelement aus, das Sie anpassen möchten. Um die Parameter für weitere Steuerelemente anzupassen, wählen Sie Zusätzliche Steuerung anpassen.
3. Überprüfen Sie im Abschnitt Konten die Konten oder OUs die Konten, auf die Sie die Richtlinie anwenden möchten.
4. Wählen Sie Weiter aus.
5. Überprüfe deine Änderungen und vergewissere dich, dass sie korrekt sind. Wenn Sie fertig sind, wählen Sie Richtlinie speichern und anwenden. In Ihrer Heimatregion und allen verknüpften Regionen setzt diese Aktion die vorhandenen Konfigurationseinstellungen der Konten außer Kraft OUs , die mit dieser Konfigurationsrichtlinie verknüpft sind. Konten und OUs können durch direkte Anwendung oder Vererbung von einem Elternteil mit einer Konfigurationsrichtlinie verknüpft werden.

Security Hub CSPM API

Zum Anpassen von Steuerparameterwerten in mehreren Konten und Regionen (API)

Um eine neue Konfigurationsrichtlinie mit benutzerdefinierten Steuerparameterwerten zu erstellen

1. Rufen Sie die [CreateConfigurationPolicy](#) API über das delegierte Administratorkonto in der Heimatregion auf.
2. Geben Sie für das `SecurityControlCustomParameters` Objekt die ID der einzelnen Steuerelemente an, die Sie anpassen möchten.
3. Geben Sie für das `Parameters` Objekt den Namen jedes Parameters an, den Sie anpassen möchten. Geben Sie für jeden Parameter, den Sie anpassen, Folgendes `CUSTOM` an `ValueType`. Geben Sie für `Value` den Datentyp des Parameters und den benutzerdefinierten Wert an. Das `Value` Feld darf nicht leer sein, wenn `ValueType` es leer ist `CUSTOM`. Wenn Ihre Anfrage einen Parameter auslöst, den das Steuerelement

unterstützt, behält dieser Parameter seinen aktuellen Wert bei. Sie können unterstützte Parameter, Datentypen und gültige Werte für ein Steuerelement finden, indem Sie die [GetSecurityControlDefinition](#)API aufrufen.

Um die Werte der Steuerparameter in einer vorhandenen Konfigurationsrichtlinie anzupassen

1. Rufen Sie die [UpdateConfigurationPolicy](#)API über das delegierte Administratorkonto in der Heimatregion auf.
2. Geben Sie für das Identifier Feld den Amazon-Ressourcennamen (ARN) oder die ID der Konfigurationsrichtlinie ein, die Sie aktualisieren möchten.
3. Geben Sie für das SecurityControlCustomParameters Objekt die ID jedes Steuerelements an, das Sie anpassen möchten.
4. Geben Sie für das Parameters Objekt den Namen jedes Parameters an, den Sie anpassen möchten. Geben Sie für jeden Parameter, den Sie anpassen, Folgendes CUSTOM anValueType. Geben Sie für Value den Datentyp des Parameters und den benutzerdefinierten Wert an. Wenn in Ihrer Anfrage ein Parameter weggelassen wird, den das Steuerelement unterstützt, behält dieser Parameter seinen aktuellen Wert bei. Sie können unterstützte Parameter, Datentypen und gültige Werte für ein Steuerelement finden, indem Sie die [GetSecurityControlDefinition](#)API aufrufen.

Mit dem folgenden AWS CLI Befehl wird beispielsweise eine neue Konfigurationsrichtlinie mit einem benutzerdefinierten Wert für den daysToExpiration Parameter von ACM.1 erstellt. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--name "SampleConfigurationPolicy" \
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
"EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0","arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0"], "SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
"SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
{"daysToExpiration": {"ValueType": "CUSTOM", "Value": "Integer": 15}}]}}}'
```


Anpassen der Steuerparameter in einem einzigen Konto und einer Region

Wenn Sie keine zentrale Konfiguration verwenden oder über ein selbstverwaltetes Konto verfügen, können Sie die Steuerparameter für Ihr Konto jeweils nur in einer Region anpassen.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten zur Anpassung der Steuerparameter. Ihre Änderungen gelten nur für Ihr Konto in der aktuellen Region. Um die Steuerungsparameter in weiteren Regionen anzupassen, wiederholen Sie die folgenden Schritte für jedes weitere Konto und jede Region, in der Sie die Parameter anpassen möchten. Das gleiche Steuerelement kann in verschiedenen Regionen unterschiedliche Parameterwerte verwenden.

Security Hub CSPM console

Um die Werte der Steuerparameter in einem Konto und einer Region (Konsole) anzupassen

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Controls aus. Wählen Sie in der Tabelle ein Steuerelement aus, das benutzerdefinierte Parameter unterstützt und für das Sie die Parameter ändern möchten. In der Spalte Benutzerdefinierte Parameter wird angegeben, welche Steuerelemente benutzerdefinierte Parameter unterstützen.
3. Wählen Sie auf der Detailseite für das Steuerelement die Registerkarte Parameter und dann Bearbeiten aus.
4. Geben Sie die gewünschten Parameterwerte an.
5. Wählen Sie optional im Abschnitt Grund für die Änderung einen Grund für die Anpassung der Parameter aus.
6. Wählen Sie Speichern.

Security Hub CSPM API

Um die Werte der Steuerparameter in einem Konto und einer Region (API) anzupassen

1. Rufen Sie die [UpdateSecurityControl](#)API auf.
2. Geben Sie für SecurityControlId die ID des Steuerelements an, das Sie anpassen möchten.
3. Geben Sie für das Parameters Objekt den Namen jedes Parameters an, den Sie anpassen möchten. Geben Sie für jeden Parameter, den Sie anpassen, Folgendes

CUSTOM anValueType. Geben Sie für Value den Datentyp des Parameters und den benutzerdefinierten Wert an. Wenn in Ihrer Anfrage ein Parameter weggelassen wird, den das Steuerelement unterstützt, behält dieser Parameter seinen aktuellen Wert bei. Sie können unterstützte Parameter, Datentypen und gültige Werte für ein Steuerelement finden, indem Sie die [GetSecurityControlDefinition](#) API aufrufen.

4. Geben Sie optional einen Grund für die Anpassung der Steuerparameter an.
LastUpdateReason

Der folgende AWS CLI Befehl definiert beispielsweise einen benutzerdefinierten Wert für den daysToExpiration Parameter von ACM.1. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub update-security-control \  
--region us-east-1 \  
--security-control-id ACM.1 \  
--parameters '{"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer":  
15}}}' \  
--last-update-reason "Internal compliance requirement"
```

Rückkehr zu den Standardwerten der Steuerparameter

Ein Steuerparameter kann einen Standardwert haben, den AWS Security Hub Cloud Security Posture Management (CSPM) definiert. Gelegentlich aktualisiert Security Hub CSPM den Standardwert für einen Parameter, um den sich entwickelnden bewährten Sicherheitsmethoden Rechnung zu tragen. Wenn Sie keinen benutzerdefinierten Wert für einen Steuerparameter angegeben haben, verfolgt das Steuerelement diese Aktualisierungen automatisch und verwendet den neuen Standardwert.

Sie können zur Verwendung der Standardparameterwerte für ein Steuerelement zurückkehren. Die Anweisungen für die Umkehrung hängen davon ab, ob Sie die [zentrale Konfiguration](#) in Security Hub CSPM verwenden. Die zentrale Konfiguration ist eine Funktion, mit der der delegierte Security Hub CSPM-Administrator die Security Hub CSPM-Funktionen für Konten und Organisationseinheiten AWS-Regionen konfigurieren kann (). OUs

 Note

Nicht alle Steuerparameter haben einen standardmäßigen Security Hub CSPM-Wert. In solchen Fällen, wenn auf gesetzt `ValueType` ist `DEFAULT`, gibt es keinen bestimmten Standardwert, den Security Hub CSPM verwendet. Stattdessen ignoriert Security Hub CSPM den Parameter, wenn kein benutzerdefinierter Wert vorhanden ist.

Rückkehr zu den Standardsteuerungsparametern in mehreren Konten und Regionen

Wenn Sie die zentrale Konfiguration verwenden, können Sie die Steuerparameter für mehrere, zentral verwaltete Konten sowie für die Heimatregion und OUs verknüpfte Regionen wiederherstellen.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um mithilfe der zentralen Konfiguration zu den Standardparameterwerten für mehrere Konten und Regionen zurückzukehren.

Security Hub CSPM console

So kehren Sie in mehreren Konten und Regionen zu den Standardwerten der Steuerparameter zurück (Konsole)

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>

Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub CSPM-Administratorkontos in der Heimatregion an.

2. Wählen Sie im Navigationsbereich Einstellungen und Konfiguration aus.
3. Wählen Sie die Registerkarte Policies.
4. Wählen Sie eine Richtlinie aus und klicken Sie dann auf Bearbeiten.
5. Unter Benutzerdefinierte Richtlinie wird im Abschnitt Steuerelemente eine Liste der Steuerelemente angezeigt, für die Sie benutzerdefinierte Parameter angegeben haben.
6. Suchen Sie das Steuerelement mit einem oder mehreren Parameterwerten, die rückgängig gemacht werden sollen. Wählen Sie dann Entfernen, um zu den Standardwerten zurückzukehren.
7. Überprüfen Sie im Abschnitt Konten die Konten oder die Konten OUs , auf die Sie die Richtlinie anwenden möchten.
8. Wählen Sie Weiter aus.

- Überprüfe deine Änderungen und vergewissere dich, dass sie korrekt sind. Wenn Sie fertig sind, wählen Sie Richtlinie speichern und anwenden. In Ihrer Heimatregion und allen verknüpften Regionen setzt diese Aktion die vorhandenen Konfigurationseinstellungen der Konten außer Kraft OUs , die mit dieser Konfigurationsrichtlinie verknüpft sind. Konten und OUs können durch direkte Anwendung oder Vererbung von einem Elternteil mit einer Konfigurationsrichtlinie verknüpft werden.

Security Hub CSPM API

Um zu den Standardwerten der Steuerparameter in mehreren Konten und Regionen zurückzukehren (API)

- Rufen Sie die [UpdateConfigurationPolicy](#) API über das delegierte Administratorkonto in der Heimatregion auf.
- Geben Sie für das Identifier Feld den Amazon-Ressourcennamen (ARN) oder die ID der Richtlinie ein, die Sie aktualisieren möchten.
- Geben Sie für das SecurityControlCustomParameters Objekt die ID jedes Steuerelements an, für das Sie einen oder mehrere Parameter rückgängig machen möchten.
- Geben Sie im Parameters Objekt für jeden Parameter, den Sie rückgängig machen möchten, das valueType Feld DEFAULT an. Wenn auf gesetzt valueType istDEFAULT, müssen Sie keinen Wert für das Value Feld angeben. Wenn in Ihrer Anfrage ein Wert enthalten ist, ignoriert Security Hub CSPM ihn. Wenn in Ihrer Anfrage ein Parameter weggelassen wird, den das Steuerelement unterstützt, behält dieser Parameter seinen aktuellen Wert bei.

Warning

Wenn Sie ein Kontrollobjekt aus dem SecurityControlCustomParameters Feld weglassen, setzt Security Hub CSPM alle benutzerdefinierten Parameter für das Steuerelement auf ihre Standardwerte zurück. Eine völlig leere Liste für SecurityControlCustomParameters setzt benutzerdefinierte Parameter für alle Steuerelemente auf ihre Standardwerte zurück.

Mit dem folgenden AWS CLI Befehl wird beispielsweise der daysToExpiration Steuerparameter für ACM.1 auf seinen Standardwert in der angegebenen Konfigurationsrichtlinie

zurückgesetzt. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--name "TestConfigurationPolicy" \
--description "Updated configuration policy" \
--updated-reason "Revert ACM.1 parameter to default value"
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
"EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0","arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
"SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
{"daysToExpiration": {"ValueType": "DEFAULT"}}]}}}]'
```

Zurücksetzen auf die Standardsteuerungsparameter in einem einzigen Konto und einer Region

Wenn Sie keine zentrale Konfiguration verwenden oder über ein selbstverwaltetes Konto verfügen, können Sie für Ihr Konto in jeweils einer Region wieder die Standardparameterwerte verwenden.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um zu den Standardparameterwerten für Ihr Konto in einer einzelnen Region zurückzukehren. Um in weiteren Regionen zu den Standardparameterwerten zurückzukehren, wiederholen Sie diese Schritte in jeder weiteren Region.

Note

Wenn Sie Security Hub CSPM deaktivieren, werden Ihre benutzerdefinierten Steuerungsparameter zurückgesetzt. Wenn Sie Security Hub CSPM in future erneut aktivieren, verwenden alle Steuerelemente beim Start Standardparameterwerte.

Security Hub CSPM console

Um zu den Standardwerten der Steuerparameter in einem Konto und einer Region (Konsole) zurückzukehren

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Controls aus. Wählen Sie das Steuerelement aus, für das Sie die Standardparameterwerte wiederherstellen möchten.
3. Wählen Sie auf der **Parameters** Registerkarte neben einem Steuerparameter die Option Benutzerdefiniert aus. Wählen Sie dann Anpassung entfernen aus. Dieser Parameter verwendet jetzt den standardmäßigen Security Hub CSPM-Wert und verfolgt future Updates auf den Standardwert.
4. Wiederholen Sie den vorherigen Schritt für jeden Parameterwert, den Sie wiederherstellen möchten.

Security Hub CSPM API

Um zu den Standardwerten der Steuerparameter in einem Konto und einer Region (API) zurückzukehren

1. Rufen Sie die API auf [UpdateSecurityControl](#).
2. Geben Sie für SecurityControlId den ARN oder die ID des Steuerelements an, dessen Parameter Sie rückgängig machen möchten.
3. Geben Sie im Parameters Objekt für jeden Parameter, den Sie rückgängig machen möchten, das ValueType Feld DEFAULT an. Wenn auf gesetzt ValueType istDEFAULT, müssen Sie keinen Wert für das Value Feld angeben. Wenn in Ihrer Anfrage ein Wert enthalten ist, ignoriert Security Hub CSPM ihn.
4. Geben Sie optional für LastUpdateReason einen Grund für die Rückkehr zu den Standardparameterwerten an.

Mit dem folgenden AWS CLI Befehl wird beispielsweise der daysToExpiration Steuerparameter für ACM.1 auf seinen Standardwert zurückgesetzt. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub update-security-control \  
--region us-east-1 \  
--security-control-id ACM.1 \  
--parameters '{"daysToExpiration": {"ValueType": "DEFAULT"}}' \  
--last-update-reason "New internal requirement"
```

Überprüfung des Status von Änderungen der Steuerparameter

Wenn Sie versuchen, einen Steuerparameter anzupassen oder den Standardwert wiederherzustellen, können Sie überprüfen, ob die gewünschten Änderungen wirksam waren. Dadurch wird sichergestellt, dass ein Steuerelement erwartungsgemäß funktioniert und den gewünschten Sicherheitswert bietet. Wenn ein Parameter-Update nicht erfolgreich ist, behält Security Hub CSPM den aktuellen Wert für den Parameter bei.

Um zu überprüfen, ob ein Parameter-Update erfolgreich war, können Sie die Details der Steuerung auf der Security Hub CSPM-Konsole überprüfen. Wählen Sie auf der Konsole im Navigationsbereich Controls aus. Wählen Sie dann ein Steuerelement aus, um dessen Details anzuzeigen. Auf der Registerkarte Parameter wird der Status der Parameteränderung angezeigt.

Wenn Ihre Anfrage zur Aktualisierung eines Parameters gültig ist, ist der Wert des `UpdateStatus` Felds programmgesteuert eine Antwort auf den [BatchGetSecurityControls](#) Vorgang. `UPDATING` Das bedeutet, dass die Aktualisierung gültig war, aber möglicherweise noch nicht alle Ergebnisse die aktualisierten Parameterwerte enthalten. Wenn sich der Wert von `UpdateState` ändert `READY`, verwendet Security Hub CSPM die aktualisierten Steuerparameterwerte bei der Ausführung von Sicherheitsprüfungen des Steuerelements. Zu den Ergebnissen gehören die aktualisierten Parameterwerte.

Die `UpdateSecurityControl` Operation gibt eine `InvalidInputException` Antwort für ungültige Parameterwerte zurück. Die Antwort enthält zusätzliche Details zur Ursache des Fehlers. Möglicherweise haben Sie einen Wert angegeben, der außerhalb des gültigen Bereichs für einen Parameter liegt. Oder Sie haben möglicherweise einen Wert angegeben, der nicht den richtigen Datentyp verwendet. Senden Sie Ihre Anfrage erneut mit einer gültigen Eingabe.

Wenn beim Versuch, einen Parameterwert zu aktualisieren, ein interner Fehler auftritt, versucht Security Hub CSPM es automatisch erneut, sofern Sie es aktiviert haben. AWS Config Weitere Informationen finden Sie unter [Überlegungen vor der Aktivierung und Konfiguration AWS Config](#).

Überprüfung und Verwaltung der Kontrollergebnisse in Security Hub CSPM

Auf der Seite mit den Kontrolldetails wird eine Liste der aktiven Ergebnisse für eine Kontrolle angezeigt. Die Liste enthält keine archivierten Ergebnisse.

Die Seite mit den Kontrolldetails unterstützt die regionsübergreifende Aggregation. Wenn Sie eine Aggregationsregion festgelegt haben, enthalten der Kontrollstatus und die Liste der Sicherheitsüberprüfungen auf der Seite mit den Kontrolldetails die Prüfungen aller verknüpften Kontrollen. AWS-Regionen

Die Liste enthält Tools zum Filtern und Sortieren der Ergebnisse, sodass Sie sich zuerst auf dringendere Ergebnisse konzentrieren können. Ein Ergebnis kann Links zu Ressourcendetails in der entsprechenden Servicekonsole enthalten. Bei Steuerelementen, die auf AWS Config Regeln basieren, können Sie sich Details zu der Regel anzeigen lassen.

Sie können auch die AWS Security Hub Cloud Security Posture Management (CSPM) -API verwenden, um eine Liste mit Ergebnissen und Ergebnisdetails abzurufen.

Weitere Informationen finden Sie unter [Details und Verlauf der Ergebnisse überprüfen](#).

Um den aktuellen Status Ihrer Untersuchung eines Kontrollbefundes widerzuspiegeln, legen Sie den Workflow-Status fest. Weitere Informationen finden Sie unter [the section called “Den Workflow-Status von Ergebnissen festlegen”](#).

Sie können auch ausgewählte Security Hub CSPM-Ergebnisse an eine benutzerdefinierte Aktion in Amazon senden. EventBridge Weitere Informationen finden Sie unter [the section called “Senden von Ergebnissen an eine benutzerdefinierte Aktion”](#).

Themen

- [Filterung und Sortierung der Kontrollergebnisse](#)
- [Stichproben von Kontrollbefunden](#)

Filterung und Sortierung der Kontrollergebnisse

Wenn Sie ein Steuerelement auf der Kontrollseite der AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole oder auf der Detailseite eines Standards auswählen, gelangen Sie zur Seite mit den Kontrolldetails.

Auf der Seite mit den Kontrolldetails werden der Titel und die Beschreibung der Kontrolle, der allgemeine Kontrollstatus und eine Aufschlüsselung der Sicherheitsüberprüfungen für die Kontrolle in den letzten 24 Stunden angezeigt.

Verwenden Sie die Option „Nach filtern“ neben der Liste der Kontrollprüfungen, um sich schnell auf Ergebnisse mit einem bestimmten [Workflow](#) - oder [Compliance-Status](#) zu konzentrieren.

Zusätzlich zu den Optionen Filtern nach können Sie das Feld Filter hinzufügen verwenden, um die Prüfliste nach anderen Feldern wie AWS-Konto ID oder Ressourcen-ID zu filtern.

Standardmäßig werden Ergebnisse mit dem Konformitätsstatus BESTANDEN zuerst aufgeführt. Sie können die Standardsortierung ändern, indem Sie in den Spaltenüberschriften eine andere Option auswählen.

Auf der Seite mit den Kontrolldetails können Sie Herunterladen wählen, um die aktuelle Seite mit den Kontrollergebnissen in eine CSV-Datei herunterzuladen.

Wenn Sie die Ergebnisliste filtern, umfasst der Download nur die Steuerelemente, die dem Filter entsprechen. Wenn Sie bestimmte Ergebnisse aus der Liste auswählen, enthält der Download nur die ausgewählten Ergebnisse.

Weitere Informationen zum Filtern von Ergebnissen finden Sie unter [Ergebnisse im Security Hub CSPM filtern](#).

Stichproben von Kontrollbefunden

Die folgenden Beispiele enthalten Beispiele für Ergebnisse der AWS Security Hub Cloud Security Posture Management (CSPM) -Steuerung im AWS Security Finding Format (ASFF). Der Inhalt der Kontrollergebnisse hängt davon ab, ob Sie die konsolidierten Kontrollergebnisse aktiviert haben.

Wenn Sie konsolidierte Kontrollergebnisse aktivieren, generiert Security Hub CSPM ein einzelnes Ergebnis für eine Kontrolle, auch wenn die Kontrolle für mehrere aktivierte Standards gilt. Wenn Sie diese Funktion nicht aktivieren, generiert Security Hub CSPM für jeden aktivierten Standard, für den ein Steuerelement gilt, einen separaten Kontrollbefund. Wenn Sie beispielsweise zwei Standards aktivieren und eine Kontrolle für beide gilt, erhalten Sie zwei separate Ergebnisse für die Kontrolle, einen für jeden Standard. Wenn Sie konsolidierte Kontrollergebnisse aktivieren, erhalten Sie nur ein Ergebnis für die Kontrolle. Weitere Informationen finden Sie unter [Konsolidierte Kontrollergebnisse](#).

Die Beispiele auf dieser Seite enthalten Beispiele für beide Szenarien. Zu den Stichproben gehören: Kontrollergebnisse für einzelne Security Hub CSPM-Standards, wenn konsolidierte

Kontrollergebnisse deaktiviert sind, und Kontrollbefunde für mehrere Security Hub CSPM-Standards, wenn konsolidierte Kontrollergebnisse aktiviert sind.

Stichproben von Kontrollbefunden

- [Ein Musterergebnis für den Standard „Bewährte Methoden für AWS grundlegende Sicherheit“](#)
- [Beispielbefund für CIS AWS Foundations Benchmark v3.0.0](#)
- [Stichprobenergebnis für CIS AWS Foundations Benchmark v1.4.0](#)
- [Ergebnis eines Beispiels für CIS AWS Foundations Benchmark v1.2.0](#)
- [Stichprobenergebnis für den Standard NIST SP 800-53 Revision 5](#)
- [Stichprobenergebnis für den Standard NIST SP 800-171 Revision 2](#)
- [Ergebnis eines Beispiels für den Datensicherheitsstandard v3.2.1 der Payment Card Industry](#)
- [Musterbefund für den AWS Resource Tagging-Standard](#)
- [Stichprobenergebnis für den AWS Control Tower Service-Managed-Standard](#)
- [Stichprobe: konsolidiertes Ergebnis für mehrere Standards](#)

Note

Die Kontrollergebnisse beziehen sich auf verschiedene Felder und Werte in den Regionen China und den AWS GovCloud (US) Regionen. Weitere Informationen finden Sie unter [Auswirkungen der Konsolidierung auf ASFF-Felder und -Werte](#).

Ein Musterergebnis für den Standard „Bewährte Methoden für AWS grundlegende Sicherheit“

Das folgende Beispiel enthält ein Beispiel für ein Ergebnis für ein Steuerelement, das für den FSBP-Standard (AWS Foundational Security Best Practices) gilt. In diesem Beispiel ist die Option „Consolidated Control Findings“ deaktiviert.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
```

```

"CompanyName": "AWS",
"Region": "us-east-2",
"GeneratorId": "aws-foundational-security-best-practices/v/1.0.0/CloudTrail.2",
"AwsAccountId": "123456789012",
"Types": [
  "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
],
"FirstObservedAt": "2020-08-06T02:18:23.076Z",
"LastObservedAt": "2021-09-28T16:10:06.956Z",
"CreatedAt": "2020-08-06T02:18:23.076Z",
"UpdatedAt": "2021-09-28T16:10:00.093Z",
"Severity": {
  "Product": 40,
  "Label": "MEDIUM",
  "Normalized": 40,
  "Original": "MEDIUM"
},
"Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
"Description": "This AWS control checks whether AWS CloudTrail is configured to use
the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
"Remediation": {
  "Recommendation": {
    "Text": "For directions on how to correct this issue, consult the AWS Security
Hub Cloud Security Posture Management (CSPM) controls documentation.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
  }
},
"ProductFields": {
  "StandardsArn": "arn:aws:securityhub::standards/aws-foundational-security-best-
practices/v/1.0.0",
  "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0",
  "ControlId": "CloudTrail.2",
  "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
  "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
  "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
  "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
  "aws/securityhub/ProductName": "Security Hub CSPM",
  "aws/securityhub/CompanyName": "AWS",

```

```

    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/aws-foundation-best-practices/v/1.0.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
    ]
  }
}

```

Beispielbefund für CIS AWS Foundations Benchmark v3.0.0

Das folgende Beispiel enthält ein Beispiel für ein Ergebnis für ein Steuerelement, das für CIS AWS Foundations Benchmark v3.0.0 gilt. In diesem Beispiel sind konsolidierte Kontrollergebnisse deaktiviert.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/3.0.0/2.2.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS Foundations Benchmark"
  ],
  "FirstObservedAt": "2024-04-18T07:46:18.193Z",
  "LastObservedAt": "2024-04-23T07:47:01.137Z",
  "CreatedAt": "2024-04-18T07:46:18.193Z",
  "UpdatedAt": "2024-04-23T07:46:46.165Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "2.2.1 EBS default encryption should be enabled",
  "Description": "Elastic Compute Cloud (EC2) supports encryption at rest when using the Elastic Block Store (EBS) service. While disabled by default, forcing encryption at EBS volume creation is supported.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security Hub Cloud Security Posture Management (CSPM) controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.7/remediation"
    }
  },
  "ProductFields": {
```

```

    "StandardsArn": "arn:aws:securityhub::standards/cis-aws-foundations-benchmark/
v/3.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/3.0.0",
    "ControlId": "2.2.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/EC2.7/
remediation",
    "RelatedAWSResources:0/name": "securityhub-ec2-ebs-encryption-by-default-2843ed9e",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/3.0.0/2.2.1",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "EBS Encryption by default is not enabled.",
    "Resources:0/Id": "arn:aws:iam::123456789012:root",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c"
  },
  "Resources": [
    {
      "Type": "AwsAccount",
      "Id": "AWS:::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v3.0.0/2.2.1"
    ],
    "SecurityControlId": "EC2.7",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/cis-aws-foundations-benchmark/v/3.0.0"
      }
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",

```

```

    "FindingProviderFields": {
      "Severity": {
        "Label": "MEDIUM",
        "Original": "MEDIUM"
      },
      "Types": [
        "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS Foundations Benchmark"
      ]
    },
    "ProcessedAt": "2024-04-23T07:47:07.088Z"
  }
}

```

Stichprobenergebnis für CIS AWS Foundations Benchmark v1.4.0

Das folgende Beispiel enthält ein Beispiel für ein Ergebnis für ein Steuerelement, das für CIS AWS Foundations Benchmark v1.4.0 gilt. In diesem Beispiel sind konsolidierte Kontrollergebnisse deaktiviert.

```

{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/1.4.0/3.7",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS Foundations Benchmark"
  ],
  "FirstObservedAt": "2022-10-21T22:14:48.913Z",
  "LastObservedAt": "2022-12-22T22:24:56.980Z",
  "CreatedAt": "2022-10-21T22:14:48.913Z",
  "UpdatedAt": "2022-12-22T22:24:52.409Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
}

```

```

    "Title": "3.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
    "Description": "AWS CloudTrail is a web service that records AWS API calls for an
account and makes those logs available to users and resources in accordance with IAM
policies. AWS Key Management Service (KMS) is a managed service that helps create
and control the encryption keys used to encrypt account data, and uses Hardware
Security Modules (HSMs) to protect the security of encryption keys. CloudTrail logs
can be configured to leverage server side encryption (SSE) and AWS KMS customer
created master keys (CMK) to further protect CloudTrail logs. It is recommended that
CloudTrail be configured to use SSE-KMS.",
    "Remediation": {
        "Recommendation": {
            "Text": "For directions on how to correct this issue, consult the AWS Security
Hub Cloud Security Posture Management (CSPM) controls documentation.",
            "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
        }
    },
    "ProductFields": {
        "StandardsArn": "arn:aws:securityhub::standards/cis-aws-foundations-benchmark/
v/1.4.0",
        "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/1.4.0",
        "ControlId": "3.7",
        "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
        "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-855f82d1",
        "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
        "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/1.4.0/3.7",
        "aws/securityhub/ProductName": "Security Hub CSPM",
        "aws/securityhub/CompanyName": "AWS",
        "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-
D0-NOT-EDIT",
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
    },
    "Resources": [
        {
            "Type": "AwsCloudTrailTrail",
            "Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-D0-NOT-
EDIT",
            "Partition": "aws",
            "Region": "us-east-1"
        }
    ]

```



```

    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v1.4.0/3.7"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
Foundations Benchmark"
    ]
  }
}

```

Ergebnis eines Beispiels für CIS AWS Foundations Benchmark v1.2.0

Das folgende Beispiel enthält ein Beispiel für ein Ergebnis für ein Steuerelement, das für CIS AWS Foundations Benchmark v1.2.0 gilt. In diesem Beispiel sind konsolidierte Kontrollergebnisse deaktiviert.

```

{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-foundations-
benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-2",

```

```

"GeneratorId": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.7",
"AwsAccountId": "123456789012",
"Types": [
  "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS Foundations Benchmark"
],
"FirstObservedAt": "2020-08-29T04:10:06.337Z",
"LastObservedAt": "2021-09-28T16:10:05.350Z",
"CreatedAt": "2020-08-29T04:10:06.337Z",
"UpdatedAt": "2021-09-28T16:10:00.087Z",
"Severity": {
  "Product": 40,
  "Label": "MEDIUM",
  "Normalized": 40,
  "Original": "MEDIUM"
},
"Title": "2.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
>Description": "AWS Key Management Service (KMS) is a managed service that helps create and control the encryption keys used to encrypt account data, and uses Hardware Security Modules (HSMs) to protect the security of encryption keys. CloudTrail logs can be configured to leverage server side encryption (SSE) and KMS customer created master keys (CMK) to further protect CloudTrail logs. It is recommended that CloudTrail be configured to use SSE-KMS.",
"Remediation": {
  "Recommendation": {
    "Text": "For directions on how to correct this issue, consult the AWS Security Hub Cloud Security Posture Management (CSPM) controls documentation.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
  }
},
"ProductFields": {
  "StandardsGuideArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0",
  "StandardsGuideSubscriptionArn": "arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-foundations-benchmark/v/1.2.0",
  "RuleId": "2.7",
  "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation",
  "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-fe95bf3f",
  "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
  "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/cis-aws-foundations-benchmark/v/1.2.0/2.7",

```

```

    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
Foundations Benchmark"
    ]
  }
}

```

Stichprobenergebnis für den Standard NIST SP 800-53 Revision 5

Das folgende Beispiel enthält ein Beispiel für ein Ergebnis für eine Kontrolle, die für den Standard NIST SP 800-53 Revision 5 gilt. In diesem Beispiel sind konsolidierte Kontrollergebnisse deaktiviert.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/v/5.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "nist-800-53/v/5.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2023-02-17T14:22:46.726Z",
  "LastObservedAt": "2023-02-17T14:22:50.846Z",
  "CreatedAt": "2023-02-17T14:22:46.726Z",
  "UpdatedAt": "2023-02-17T14:22:46.726Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to fix this issue, consult the AWS Security Hub Cloud Security Posture Management (CSPM) NIST 800-53 R5 documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/nist-800-53/v/5.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/v/5.0.0",
  }
}
```

```

    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.9/remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/Product Name": "Security Hub CSPM",
    "aws/securityhub/Company Name": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-D0-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/v/5.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",

      "Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/AWS MacieTrail-D0-NOT-EDIT",

      "Partition": "aws",

      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "NIST.800-53.r5 AU-9",
      "NIST.800-53.r5 CA-9(1)",
      "NIST.800-53.r5 CM-3(6)",
      "NIST.800-53.r5 SC-13",
      "NIST.800-53.r5 SC-28",
      "NIST.800-53.r5 SC-28(1)",
      "NIST.800-53.r5 SC-7(10)",
      "NIST.800-53.r5 SI-7(6)"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/nist-800-53/v/5.0.0"
      }
    ]
  }
}

```

```

    }
  ]
},
"WorkflowState": "NEW",
"Workflow": {
  "Status": "NEW"
},
"RecordState": "ACTIVE",
"FindingProviderFields": {
  "Severity": {
    "Label": "MEDIUM",
    "Original": "MEDIUM"
  },
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ]
},
"ProcessedAt": "2023-02-17T14:22:53.572Z"
}

```

Stichprobenergebnis für den Standard NIST SP 800-171 Revision 2

Das folgende Beispiel enthält ein Beispiel für ein Ergebnis für eine Kontrolle, das für den Standard NIST SP 800-171 Revision 2 gilt. In diesem Beispiel sind konsolidierte Kontrollergebnisse deaktiviert.

```

{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-171/v/2.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "nist-800-171/v/2.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "AwsAccountName": "TestAcct",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2025-05-29T05:23:58.690Z",
  "LastObservedAt": "2025-05-30T05:50:11.898Z",
  "CreatedAt": "2025-05-29T05:24:24.772Z",
  "UpdatedAt": "2025-05-30T05:50:34.292Z",
}

```

```

"Severity": {
  "Product": 40,
  "Label": "MEDIUM",
  "Normalized": 40,
  "Original": "MEDIUM"
},
"Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
"Description": "This AWS control checks whether AWS CloudTrail is configured to use the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
"Remediation": {
  "Recommendation": {
    "Text": "For information on how to correct this issue, consult the AWS Security Hub Cloud Security Posture Management (CSPM) controls documentation.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
  }
},
"ProductFields": {
  "StandardsArn": "arn:aws:securityhub::standards/nist-800-171/v/2.0.0",
  "StandardsSubscriptionArn": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-171/v/2.0.0",
  "ControlId": "CloudTrail.2",
  "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation",
  "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-0ab1c2d4",
  "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
  "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/nist-800-171/v/2.0.0/CloudTrail.2",
  "aws/securityhub/ProductName": "Security Hub",
  "aws/securityhub/CompanyName": "AWS",
  "Resources:0/Id": "arn:aws:cloudtrail:ca-central-1:123456789012:trail/aws-BaselineCloudTrail",
  "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-171/v/2.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
},
"Resources": [
  {
    "Id": "arn:aws:cloudtrail:ca-central-1:123456789012:trail/aws-BaselineCloudTrail",
    "Partition": "aws",
    "Region": "us-east-1",
    "Type": "AwsCloudTrailTrail"
  }
]

```

```

    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "RelatedRequirements": [
      "NIST.800-171.r2/3.3.8"
    ],
    "AssociatedStandards": [
      {
        "StandardsId": "standards/nist-800-171/v/2.0.0"
      }
    ]
  },
  "Workflow": {
    "Status": "NEW"
  },
  "WorkflowState": "NEW",
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ],
    "Severity": {
      "Product": 40,
      "Label": "MEDIUM",
      "Normalized": 40,
      "Original": "MEDIUM"
    }
  },
  "ProcessedAt": "2025-05-30T05:50:40.297Z"
}

```

Ergebnis eines Beispiels für den Datensicherheitsstandard v3.2.1 der Payment Card Industry

Das folgende Beispiel enthält ein Beispiel für ein Ergebnis für ein Steuerelement, das für den Payment Card Industry Data Security Standard (PCI DSS) v3.2.1 gilt. In diesem Beispiel sind konsolidierte Kontrollergebnisse deaktiviert.

```

{
  "SchemaVersion": "2018-10-08",

```



```

    "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
    "ProductName": "Security Hub CSPM",
    "CompanyName": "AWS",
    "Region": "us-east-2",
    "GeneratorId": "pci-dss/v/3.2.1/PCI.CloudTrail.1",
    "AwsAccountId": "123456789012",
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
    ],
    "FirstObservedAt": "2020-08-06T02:18:23.089Z",
    "LastObservedAt": "2021-09-28T16:10:06.942Z",
    "CreatedAt": "2020-08-06T02:18:23.089Z",
    "UpdatedAt": "2021-09-28T16:10:00.090Z",
    "Severity": {
      "Product": 40,
      "Label": "MEDIUM",
      "Normalized": 40,
      "Original": "MEDIUM"
    },
    "Title": "PCI.CloudTrail.1 CloudTrail logs should be encrypted at rest using AWS KMS
CMKs",
    "Description": "This AWS control checks whether AWS CloudTrail is configured to use
the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
key (CMK) encryption by checking if the KmsKeyId is defined.",
    "Remediation": {
      "Recommendation": {
        "Text": "For directions on how to correct this issue, consult the AWS Security
Hub Cloud Security Posture Management (CSPM) controls documentation.",
        "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
      }
    },
    "ProductFields": {
      "StandardsArn": "arn:aws:securityhub:::standards/pci-dss/v/3.2.1",
      "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/pci-dss/v/3.2.1",
      "ControlId": "PCI.CloudTrail.1",
      "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
      "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
      "Related AWS Resources:0/type": "AWS::Config::ConfigRule",

```

```

    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/pci-dss/
v/3.2.1/PCI.CloudTrail.1",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "PCI DSS 3.4"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/pci-dss/v/3.2.1"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
    ]
  }
}

```

}

Musterbefund für den AWS Resource Tagging-Standard

Das folgende Beispiel enthält ein Beispiel für ein Ergebnis für ein Steuerelement, das für den AWS Resource Tagging-Standard gilt. In diesem Beispiel sind konsolidierte Kontrollergebnisse deaktiviert.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "eu-central-1",
  "GeneratorId": "security-control/EC2.44",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2024-02-19T21:00:32.206Z",
  "LastObservedAt": "2024-04-29T13:01:57.861Z",
  "CreatedAt": "2024-02-19T21:00:32.206Z",
  "UpdatedAt": "2024-04-29T13:01:41.242Z",
  "Severity": {
    "Label": "LOW",
    "Normalized": 1,
    "Original": "LOW"
  },
  "Title": "EC2 subnets should be tagged",
  "Description": "This control checks whether an Amazon EC2 subnet has tags with the specific keys defined in the parameter requiredTagKeys. The control fails if the subnet doesn't have any tag keys or if it doesn't have all the keys specified in the parameter requiredTagKeys. If the parameter requiredTagKeys isn't provided, the control only checks for the existence of a tag key and fails if the subnet isn't tagged with any key. System tags, which are automatically applied and begin with aws:, are ignored.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security Hub Cloud Security Posture Management (CSPM) controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.44/remediation"
    }
  }
}
```

```

},
"ProductFields": {
  "RelatedAWSResources:0/name": "securityhub-tagged-ec2-subnet-6ceafede",
  "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
  "aws/securityhub/ProductName": "Security Hub CSPM",
  "aws/securityhub/CompanyName": "AWS",
  "aws/securityhub/annotation": "No tags are present.",
  "Resources:0/Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
  "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/
securityhub/arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
},
"Resources": [
  {
    "Type": "AwsEc2Subnet",
    "Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/subnet-1234567890abcdef0",
    "Partition": "aws",
    "Region": "eu-central-1",
    "Details": {
      "AwsEc2Subnet": {
        "AssignIpv6AddressOnCreation": false,
        "AvailabilityZone": "eu-central-1b",
        "AvailabilityZoneId": "euc1-az3",
        "AvailableIpAddressCount": 4091,
        "CidrBlock": "10.24.34.0/23",
        "DefaultForAz": true,
        "MapPublicIpOnLaunch": true,
        "OwnerId": "123456789012",
        "State": "available",
        "SubnetArn": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
        "SubnetId": "subnet-1234567890abcdef0",
        "VpcId": "vpc-021345abcdef6789"
      }
    }
  }
],
"Compliance": {
  "Status": "FAILED",
  "SecurityControlId": "EC2.44",
  "AssociatedStandards": [
    {
      "StandardsId": "standards/aws-resource-tagging-standard/v/1.0.0"
    }
  ]
}

```

```

    }
  ],
  "SecurityControlParameters": [
    {
      "Name": "requiredTagKeys",
      "Value": [
        "peepoo"
      ]
    }
  ],
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "LOW",
      "Original": "LOW"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  },
  "ProcessedAt": "2024-04-29T13:02:03.259Z"
}

```

Stichprobenergebnis für den AWS Control Tower Service-Managed-Standard

Das folgende Beispiel enthält ein Beispiel für ein Ergebnis für ein Steuerelement, das für den vom AWS Control Tower Service verwalteten Standard gilt. In diesem Beispiel sind konsolidierte Kontrollergebnisse deaktiviert.

```

{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-aws-control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "service-managed-aws-control-tower/v/1.0.0/CloudTrail.2",

```

```

"AwsAccountId": "123456789012",
"Types": [
  "Software and Configuration Checks/Industry and Regulatory Standards"
],
"FirstObservedAt": "2022-11-17T01:25:30.296Z",
"LastObservedAt": "2022-11-17T01:25:45.805Z",
"CreatedAt": "2022-11-17T01:25:30.296Z",
"UpdatedAt": "2022-11-17T01:25:30.296Z",
"Severity": {
  "Product": 40,
  "Label": "MEDIUM",
  "Normalized": 40,
  "Original": "MEDIUM"
},
"Title": "CT.CloudTrail.2 CloudTrail should have encryption at-rest enabled",
"Description": "This AWS control checks whether AWS CloudTrail is configured to use the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
"Remediation": {
  "Recommendation": {
    "Text": "For information on how to correct this issue, consult the AWS Security Hub Cloud Security Posture Management (CSPM) controls documentation.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
  }
},
"ProductFields": {
  "StandardsArn": "arn:aws:securityhub::standards/service-managed-aws-control-tower/v/1.0.0",
  "StandardsSubscriptionArn": "arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-aws-control-tower/v/1.0.0",
  "ControlId": "CT.CloudTrail.2",
  "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation",
  "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-fe95bf3f",
  "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
  "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/service-managed-aws-control-tower/v/1.0.0/CloudTrail.2",
  "aws/securityhub/ProductName": "Security Hub CSPM",
  "aws/securityhub/CompanyName": "AWS",
  "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-DO-NOT-EDIT",

```

```

    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-
aws-control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsAccount",
      "Id": "AWS:::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  }
}

```

Stichprobe: konsolidiertes Ergebnis für mehrere Standards

Das folgende Beispiel enthält ein Beispiel für ein Ergebnis für ein Steuerelement, das für mehrere aktivierte Standards gilt. In diesem Beispiel sind konsolidierte Kontrollergebnisse aktiviert.

```

{
  "SchemaVersion": "2018-10-08",

```

```

    "Id": "arn:aws:securityhub:us-east-1:123456789012:security-control/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
    "ProductName": "Security Hub",
    "CompanyName": "AWS",
    "Region": "us-east-1",
    "GeneratorId": "security-control/CloudTrail.2",
    "AwsAccountId": "123456789012",
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ],
    "FirstObservedAt": "2024-08-09T14:57:04.521Z",
    "LastObservedAt": "2025-05-30T03:30:17.407Z",
    "CreatedAt": "2024-08-09T14:57:04.521Z",
    "UpdatedAt": "2025-05-30T03:30:32.781Z",
    "Severity": {
      "Label": "MEDIUM",
      "Normalized": 40,
      "Original": "MEDIUM"
    },
    "Title": "CloudTrail should have encryption at-rest enabled",
    "Description": "This AWS control checks whether AWS CloudTrail is configured to use the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
    "Remediation": {
      "Recommendation": {
        "Text": "For information on how to correct this issue, consult the AWS Security Hub Cloud Security Posture Management (CSPM) controls documentation.",
        "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
      }
    },
    "ProductFields": {
      "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-01a2b345",
      "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
      "aws/securityhub/ProductName": "Security Hub",
      "aws/securityhub/CompanyName": "AWS",
      "Resources:0/Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TestTrail-D0-NOT-DELETE",
      "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:security-control/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
    },
    "Resources": [

```



```

{
  "Type": "AwsCloudTrailTrail",
  "Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TestTrail-DO-NOT-DELETE",
  "Partition": "aws",
  "Region": "us-east-1",
  "Details": {
    "AwsCloudTrailTrail": {
      "HasCustomEventSelectors": false,
      "IncludeGlobalServiceEvents": true,
      "LogFileValidationEnabled": true,
      "HomeRegion": "us-east-1",
      "IsMultiRegionTrail": true,
      "S3BucketName": "cloudtrail-awslogs-do-not-delete",
      "IsOrganizationTrail": false,
      "Name": "TestTrail-DO-NOT-DELETE"
    }
  }
},
"Compliance": {
  "Status": "FAILED",
  "SecurityControlId": "CloudTrail.2",
  "RelatedRequirements": [
    "CIS AWS Foundations Benchmark v1.2.0/2.7",
    "CIS AWS Foundations Benchmark v1.4.0/3.7",
    "CIS AWS Foundations Benchmark v3.0.0/3.5",
    "NIST.800-171.r2/3.3.8",
    "PCI DSS v3.2.1/3.4",
    "PCI DSS v4.0.1/10.3.2"
  ],
  "AssociatedStandards": [
    { "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"},
    { "StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
    { "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"},
    { "StandardsId": "standards/cis-aws-foundations-benchmark/v/3.0.0"},
    { "StandardsId": "standards/nist-800-171/v/2.0.0"},
    { "StandardsId": "standards/pci-dss/v/3.2.1"},
    { "StandardsId": "standards/pci-dss/v/4.0.1"}
  ]
},
"Workflow": {
  "Status": "NEW"
},
"WorkflowState": "NEW",

```

```
"RecordState": "ACTIVE",
"FindingProviderFields": {
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "Severity": {
    "Normalized": 40,
    "Label": "MEDIUM",
    "Original": "MEDIUM"
  }
},
"ProcessedAt": "2025-05-30T03:31:00.831Z"
}
```

Integrationen in Security Hub CSPM verstehen

AWS Security Hub Cloud Security Posture Management (CSPM) kann Sicherheitsergebnisse von verschiedenen AWS-Services und unterstützten Sicherheitslösungen von Drittanbietern AWS Partner Network aufnehmen. Diese Integrationen können Ihnen helfen, sich einen umfassenden Überblick über Sicherheit und Compliance in Ihrer gesamten Umgebung zu verschaffen. AWS Security Hub CSPM nimmt Erkenntnisse aus integrierten Lösungen auf und konvertiert sie in das AWS Security Finding Format (ASFF).

Important

Bei unterstützten Produktintegrationen AWS und Integrationen von Drittanbietern empfängt und konsolidiert Security Hub CSPM die Ergebnisse, die erst generiert werden, nachdem Sie Security Hub CSPM für Ihren aktiviert haben. AWS-Konten Der Service empfängt und konsolidiert nicht rückwirkend Sicherheitserkenntnisse, die vor der Aktivierung von Security Hub CSPM generiert wurden.

Die Seite Integrationen der Security Hub CSPM-Konsole bietet Zugriff auf verfügbare Produktintegrationen AWS und Produktintegrationen von Drittanbietern. Die Security Hub CSPM-API bietet auch Funktionen zur Verwaltung von Integrationen.

Eine Integration ist möglicherweise nicht in allen verfügbar. AWS-Regionen Wenn eine Integration in der Region, in der Sie derzeit angemeldet sind, auf der Security Hub CSPM-Konsole nicht unterstützt wird, wird sie nicht auf der Integrationsseite der Konsole angezeigt. Eine Liste der Integrationen, die in den Regionen China und verfügbar sind AWS GovCloud (US) Regions, finden Sie unter [Verfügbarkeit von Integrationen nach Regionen](#).

Zusätzlich zu den AWS-Service integrierten Integrationen von Drittanbietern können Sie benutzerdefinierte Sicherheitsprodukte in Security Hub CSPM integrieren. Anschließend können Sie die Ergebnisse dieser Produkte mithilfe der Security Hub CSPM-API an Security Hub CSPM senden. Sie können die API auch verwenden, um bestehende Ergebnisse zu aktualisieren, die Security Hub CSPM von einem benutzerdefinierten Sicherheitsprodukt erhalten hat.

Themen

- [Überprüfung einer Liste der Security Hub CSPM-Integrationen](#)
- [Den Fluss von Erkenntnissen aus einer Security Hub CSPM-Integration ermöglichen](#)

- [Deaktivierung des Erkenntnisflusses aus einer Security Hub CSPM-Integration](#)
- [Ergebnisse einer Security Hub CSPM-Integration anzeigen](#)
- [AWS-Service Integrationen mit Security Hub CSPM](#)
- [Produktintegrationen von Drittanbietern mit Security Hub CSPM](#)
- [Integration von Security Hub CSPM mit kundenspezifischen Produkten](#)

Überprüfung einer Liste der Security Hub CSPM-Integrationen

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um eine Liste der Integrationen in AWS Security Hub Cloud Security Posture Management (CSPM) oder Details zu einer bestimmten Integration einzusehen.

Security Hub CSPM console

Um die Integrationsoptionen und Details zu überprüfen (Konsole)

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Security Hub CSPM-Navigationsbereich Integrationen aus.

Auf der Seite Integrationen AWS-Services werden Integrationen mit anderen zuerst aufgeführt, gefolgt von Integrationen mit Produkten von Drittanbietern.

Für jede Integration enthält die Seite Integrationen die folgenden Informationen:

- Der Name des Unternehmens
- Der Name des Produkts.
- Eine Beschreibung der Integration.
- Die Kategorien, für die die Integration gilt
- So aktivieren Sie die Integration:
- Der aktuelle Status der Integration

Sie können die Liste filtern, indem Sie Text aus den folgenden Feldern eingeben:

- Unternehmensname

- Produktname
- Beschreibung der Integration
- Kategorien

Security Hub CSPM API

Um die Integrationsoptionen und Details (API) zu überprüfen

Verwenden Sie den [DescribeProducts](#)Vorgang, um eine Liste der Integrationen zu erhalten. Wenn Sie den verwenden AWS CLI, führen Sie den [describe-products](#)Befehl aus.

Um Details für eine bestimmte Produktintegration abzurufen, verwenden Sie den `ProductArn` Parameter, um den Amazon-Ressourcennamen (ARN) der Integration anzugeben.

Mit dem folgenden AWS CLI Befehl werden beispielsweise Details zur Security Hub CSPM-Integration mit 3 abgerufen. CORESec

```
$ aws securityhub describe-products --product-arn "arn:aws:securityhub:us-east-1::product/3coresec/3coresec"
```

Den Fluss von Erkenntnissen aus einer Security Hub CSPM-Integration ermöglichen

Auf der Seite Integrationen der AWS Security Hub Cloud Security Posture Management (CSPM) - Konsole sehen Sie die erforderlichen Schritte, um die einzelnen Integrationen zu aktivieren.

Bei den meisten Integrationen mit anderen AWS-Services ist der einzige erforderliche Schritt zur Aktivierung der Integration die Aktivierung des anderen Dienstes. Die Integrationsinformationen enthalten einen Link zur Homepage des anderen Dienstes. Wenn Sie den anderen Dienst aktivieren, wird automatisch eine Berechtigung auf Ressourcenebene erstellt und angewendet, die es Security Hub CSPM ermöglicht, Ergebnisse von dem Dienst zu empfangen.

Bei Produktintegrationen von Drittanbietern müssen Sie die Integration möglicherweise bei der erwerben und anschließend AWS Marketplace konfigurieren. Die Integrationsinformationen enthalten Links zur Ausführung dieser Aufgaben.

Wenn mehrere Versionen eines Produkts verfügbar sind AWS Marketplace, wählen Sie die Version aus, die Sie abonnieren möchten, und klicken Sie dann auf Weiter abonnieren. Einige Produkte bieten beispielsweise eine Standardversion und eine AWS GovCloud (US) Version an.

Wenn Sie eine Produktintegration aktivieren, wird dem Produktabonnement automatisch eine Ressourcenrichtlinie angefügt. Diese Ressourcenrichtlinie definiert die Berechtigungen, die Security Hub CSPM benötigt, um Ergebnisse aus diesem Produkt zu erhalten.

Nachdem Sie alle vorbereitenden Schritte zur Aktivierung einer Integration abgeschlossen haben, können Sie den Fluss der Ergebnisse aus dieser Integration deaktivieren und wieder aktivieren. Bei Integrationen, die Ergebnisse senden, geben die Statusinformationen auf der Seite Integrationen an, ob Sie derzeit Ergebnisse akzeptieren.

Security Hub CSPM console

Um den Fluss von Erkenntnissen aus einer Integration (Konsole) zu ermöglichen

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Security Hub CSPM-Navigationsbereich Integrationen aus.
3. Bei Integrationen, die Ergebnisse senden, geben die Statusinformationen an, ob Security Hub CSPM derzeit Ergebnisse aus dieser Integration akzeptiert.
4. Wählen Sie Ergebnisse akzeptieren aus.

Security Hub CSPM API

Verwenden Sie die [EnableImportFindingsForProduct](#) Operation. Wenn Sie den verwenden AWS CLI, führen Sie den [enable-import-findings-for-product](#) Befehl aus. Damit Security Hub Ergebnisse aus einer Integration empfangen kann, benötigen Sie das Produkt ARN. Verwenden Sie den [DescribeProducts](#) Vorgang, um die ARNs für die verfügbaren Integrationen abzurufen. Wenn Sie den verwenden AWS CLI, führen Sie den aus. [describe-products](#)

Mit dem folgenden AWS CLI Befehl kann Security Hub CSPM beispielsweise Ergebnisse aus der CrowdStrike Falcon-Integration empfangen. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub enable-import-findings-for product --product-arn  
"arn:aws:securityhub:us-east-1:123456789333:product/crowdstrike/crowdstrike-falcon"
```

Deaktivierung des Erkenntnisflusses aus einer Security Hub CSPM-Integration

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um den Fluss der Ergebnisse aus einer AWS Security Hub Cloud Security Posture Management (CSPM) -Integration zu deaktivieren.

Security Hub CSPM console

Um den Fluss der Ergebnisse aus einer Integration (Konsole) zu deaktivieren

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Security Hub CSPM-Navigationsbereich Integrationen aus.
3. Bei Integrationen, die Ergebnisse senden, geben die Statusinformationen an, ob Security Hub CSPM derzeit Ergebnisse aus dieser Integration akzeptiert.
4. Wählen Sie Beenden der Annahme von Ergebnissen aus.

Security Hub CSPM API

Verwenden Sie die [DisableImportFindingsForProduct](#)Operation. Wenn Sie den verwenden AWS CLI, führen Sie den [disable-import-findings-for-product](#)Befehl aus. Um den Fluss der Ergebnisse einer Integration zu deaktivieren, benötigen Sie den Abonnement-ARN für die aktivierte Integration. Verwenden Sie den [ListEnabledProductsForImport](#)Vorgang, um den Abonnement-ARN zu erhalten. Wenn Sie den verwenden AWS CLI, führen Sie den aus [list-enabled-products-for-import](#).

Der folgende AWS CLI Befehl deaktiviert beispielsweise den Fluss von Ergebnissen aus der Falcon-Integration an Security Hub CSPM. CrowdStrike Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub disable-import-findings-for-product --product-subscription-arn  
"arn:aws:securityhub:us-west-1:123456789012:product-subscription/crowdstrike/  
crowdstrike-falcon"
```

Ergebnisse einer Security Hub CSPM-Integration anzeigen

Wenn Sie beginnen, Ergebnisse aus einer AWS Security Hub Cloud Security Posture Management (CSPM) -Integration zu akzeptieren, zeigt die Seite Integrationen der Security Hub CSPM-Konsole den Status der Integration als Ergebnisse akzeptieren an. Um eine Liste der Ergebnisse der Integration einzusehen, wählen Sie Ergebnisse anzeigen.

Die Ergebnisliste zeigt die aktiven Ergebnisse für die ausgewählte Integration mit dem Workflow-Status NEW oder NOTIFIED.

Wenn Sie die regionsübergreifende Aggregation aktivieren, enthält die Liste in der Aggregationsregion Ergebnisse aus der Aggregationsregion und aus verknüpften Regionen, in denen die Integration aktiviert ist. Security Hub aktiviert Integrationen nicht automatisch, die auf der regionsübergreifenden Aggregationskonfiguration basieren.

In anderen Regionen enthält die Ergebnisliste für eine Integration nur Ergebnisse aus der aktuellen Region.

Informationen zur Konfiguration der regionsübergreifenden Aggregation finden Sie unter [Aggregation von CSPM-Daten über Regionen hinweg](#)

In der Ergebnisliste können Sie die folgenden Aktionen ausführen.

- [Ändern der Filter und Gruppierung für die Liste](#)
- [Anzeigen der Details für einzelne Ergebnisse](#)
- [Aktualisieren des Workflow-Status der Ergebnisse](#)
- [Senden der Ergebnisse an benutzerdefinierte Aktionen](#)

AWS-Service Integrationen mit Security Hub CSPM

AWS Security Hub Cloud Security Posture Management (CSPM) unterstützt Integrationen mit mehreren anderen AWS-Services. Diese Integrationen können Ihnen helfen, sich einen umfassenden Überblick über Sicherheit und Compliance in Ihrer gesamten Umgebung zu verschaffen. AWS

Sofern unten nicht anders angegeben, werden AWS-Service Integrationen, die Ergebnisse an Security Hub CSPM senden, automatisch aktiviert, nachdem Sie Security Hub CSPM und den anderen Dienst aktiviert haben. Integrationen, die Security Hub CSPM-Ergebnisse erhalten, erfordern möglicherweise zusätzliche Schritte zur Aktivierung. Lesen Sie die Informationen zu den einzelnen Integrationen, um mehr zu erfahren.

Einige Integrationen sind nicht in allen AWS-Regionen verfügbar. Auf der Security Hub CSPM-Konsole wird eine Integration nicht auf der Seite Integrationen angezeigt, wenn sie in der aktuellen Region nicht unterstützt wird. Eine Liste der Integrationen, die in den Regionen China und verfügbar sind AWS GovCloud (US) Regions, finden Sie unter [Verfügbarkeit von Integrationen nach Regionen](#).

Überblick über die AWS Serviceintegrationen mit Security Hub CSPM

Die folgende Tabelle bietet einen Überblick über AWS Dienste, die Ergebnisse an Security Hub CSPM senden oder Ergebnisse von Security Hub CSPM empfangen.

Integrierter Service AWS	Richtung	
AWS Config	Sendet Ergebnisse	
AWS Firewall Manager	Sendet Ergebnisse	
Amazon GuardDuty	Sendet Ergebnisse	
AWS Health	Sendet Ergebnisse	
AWS Identity and Access Management Access Analyzer	Sendet Ergebnisse	
Amazon Inspector	Sendet Ergebnisse	
AWS IoT Device Defender	Sendet Ergebnisse	
Amazon Macie	Sendet Ergebnisse	
Amazon Route 53 Resolver DNS-Firewall	Sendet Ergebnisse	
AWS Systems Manager Patchmanager	Sendet Ergebnisse	
AWS Audit Manager	Empfängt Ergebnisse	
Amazon Q Developer in Chat-Anwendungen	Erhält Ergebnisse	
Amazon Detective	Erhält Ergebnisse	

Integrierter Service AWS	Richtung	
Amazon Security Lake	Erhält Ergebnisse	
AWS Systems Manager E ntdecker und OpsCenter	Empfängt und aktualisiert die Ergebnisse	
AWS Trusted Advisor	Erhält Ergebnisse	

AWS Dienste, die Ergebnisse an Security Hub CSPM senden

Die folgenden Funktionen AWS-Services lassen sich in Security Hub CSPM integrieren und können Ergebnisse an Security Hub CSPM senden. Security Hub CSPM konvertiert die Ergebnisse in das [AWS Security Finding Format](#).

AWS Config (Sendet Ergebnisse)

AWS Config ist ein Service, mit dem Sie die Konfigurationen Ihrer AWS Ressourcen bewerten, prüfen und auswerten können. AWS Config überwacht und zeichnet Ihre AWS Ressourcenkonfigurationen kontinuierlich auf und ermöglicht es Ihnen, die Auswertung der aufgezeichneten Konfigurationen anhand der gewünschten Konfigurationen zu automatisieren.

Wenn Sie die Integration mit verwenden AWS Config, können Sie die Ergebnisse AWS Config verwalteter und benutzerdefinierter Regelauswertungen als Ergebnisse in Security Hub CSPM anzeigen. Diese Ergebnisse können zusammen mit anderen CSPM-Ergebnissen von Security Hub eingesehen werden und bieten so einen umfassenden Überblick über Ihren Sicherheitsstatus.

AWS Config verwendet Amazon EventBridge , um AWS Config Regelauswertungen an Security Hub CSPM zu senden. Security Hub CSPM wandelt die Regelauswertungen in Ergebnisse um, die dem [AWS Security](#) Finding Format entsprechen. Security Hub CSPM bereichert die Ergebnisse dann nach bestem Wissen und Gewissen, indem weitere Informationen über die betroffenen Ressourcen abgerufen werden, z. B. den Amazon-Ressourcennamen (ARN), die Ressourcen-Tags und das Erstellungsdatum.

Weitere Informationen zu dieser Integration finden Sie in den folgenden Abschnitten.

Wie AWS Config sendet man Ergebnisse an Security Hub CSPM

Alle Ergebnisse in Security Hub CSPM verwenden das standardmäßige JSON-Format von ASFF. ASFF enthält Details zur Herkunft des Befundes, zur betroffenen Ressource und zum aktuellen

Status des Ergebnisses. AWS Config sendet verwaltete und benutzerdefinierte Regelauswertungen an Security Hub CSPM über. EventBridge Security Hub CSPM wandelt die Regelbeurteilungen in Ergebnisse um, die sich an ASFF orientieren, und bereichert die Ergebnisse nach bestem Wissen und Gewissen.

Arten von Ergebnissen, die AWS Config an Security Hub CSPM gesendet werden

AWS Config Sendet nach der Aktivierung der Integration Bewertungen aller AWS Config verwalteten Regeln und benutzerdefinierten Regeln an Security Hub CSPM. Es werden nur Bewertungen gesendet, die nach der Aktivierung von Security Hub CSPM durchgeführt wurden. Nehmen wir zum Beispiel an, dass bei einer AWS Config Regelauswertung fünf Ressourcen ausgefallen sind. Wenn ich danach Security Hub CSPM aktiviere und die Regel dann eine sechste ausgefallene Ressource aufdeckt, wird nur die sechste Ressourcenbewertung an Security Hub CSPM AWS Config gesendet.

Evaluierungen anhand von [serviceverknüpften AWS Config Regeln](#), wie sie beispielsweise zur Durchführung von Prüfungen von Security Hub CSPM-Steuerelementen verwendet werden, sind ausgeschlossen.

AWS Config Ergebnisse an Security Hub CSPM senden

Wenn die Integration aktiviert ist, weist Security Hub CSPM automatisch die Berechtigungen zu, die für den Empfang von Ergebnissen erforderlich sind. AWS Config Security Hub CSPM verwendet service-to-service Level-Berechtigungen, die Ihnen eine sichere Möglichkeit bieten, diese Integration zu aktivieren und Ergebnisse von AWS Config Amazon zu importieren. EventBridge

Latenz für das Senden von Erkenntnissen

Wenn ein neues Ergebnis AWS Config erstellt wird, können Sie das Ergebnis normalerweise innerhalb von fünf Minuten in Security Hub CSPM anzeigen.

Wiederholter Versuch, wenn Security Hub CSPM nicht verfügbar ist

AWS Config sendet die Ergebnisse nach bestem Wissen und Gewissen an Security Hub CSPM. EventBridge Wenn ein Ereignis nicht erfolgreich an Security Hub CSPM übermittelt wurde, wird die Zustellung bis zu 24 Stunden oder 185 Mal EventBridge wiederholt, je nachdem, was zuerst eintritt.

Aktualisierung vorhandener AWS Config Ergebnisse in Security Hub CSPM

Nachdem ein Ergebnis an Security Hub CSPM AWS Config gesendet wurde, kann es Aktualisierungen desselben Ergebnisses an Security Hub CSPM senden, um zusätzliche Beobachtungen der Findungsaktivität widerzuspiegeln. Updates werden nur für Ereignisse gesendet. ComplianceChangeNotification Wenn keine Änderung der Konformität erfolgt, werden keine

Updates an Security Hub CSPM gesendet. Security Hub CSPM löscht Ergebnisse 90 Tage nach dem letzten Update oder 90 Tage nach der Erstellung, wenn kein Update erfolgt.

Security Hub CSPM archiviert keine Ergebnisse, die gesendet werden, AWS Config selbst wenn Sie die zugehörige Ressource löschen.

Regionen, in denen Ergebnisse vorliegen AWS Config

AWS Config Die Ergebnisse erfolgen auf regionaler Basis. AWS Config sendet Ergebnisse an Security Hub CSPM in derselben Region oder Regionen, in denen die Ergebnisse auftreten.

AWS Config Ergebnisse in Security Hub CSPM anzeigen

Um Ihre AWS Config Ergebnisse anzuzeigen, wählen Sie Findings im Security Hub CSPM-Navigationsbereich aus. Um die Ergebnisse so zu filtern, dass nur AWS Config Ergebnisse angezeigt werden, wählen Sie in der Dropdownliste der Suchleiste die Option Produktname aus. Geben Sie Config ein und wählen Sie Apply aus.

Interpretieren AWS Config von gefundenen Namen in Security Hub CSPM

Security Hub CSPM wandelt AWS Config Regelauswertungen in Ergebnisse um, die dem folgen.

[AWS Format für Sicherheitssuche \(ASFF\)](#) AWS Config Regelauswertungen verwenden ein anderes Ereignismuster als ASFF. In der folgenden Tabelle werden die Felder für die AWS Config Regelauswertung ihrem ASFF-Gegenstück zugeordnet, so wie sie in Security Hub CSPM erscheinen.

Findetyp für die Auswertung der Konfigurationsregel	ASFF-Ergebnistyp	Hartcodierter Wert
Detail. awsAccountId	AwsAccountId	
Detail. newEvaluationResult. resultRecordedTime	CreatedAt	
Detail. newEvaluationResult. resultRecordedTime	UpdatedAt	
	ProductArn	<region>„arn ::securityhub:<partition>::“ product/aws/config
	ProductName	„Config“

Findetyp für die Auswertung der Konfigurationsregel	ASFF-Ergebnistyp	Hartcodierter Wert
	CompanyName	"AWS"
	Region	„eu-central-1“
configRuleArn	GeneratorId, ProductFields	
Detail. ConfigRuleARN/finding/hash	Id	
Detail. configRuleName	Titel, ProductFields	
Detail. configRuleName	Beschreibung	„Dieses Ergebnis wurde für eine Änderung der Ressource nkonformität für die Konfigurationsregel erstellt:\${detail. ConfigRuleName} “
Konfigurationselement „ARN“ oder von Security Hub CSPM berechneter ARN	Ressourcen [i] .id	
detail.Ressourcentyp	Ressourcen [i] .Type	"AwsS3Bucket"
	Ressourcen [i] .Partition	"aws"
	Ressourcen [i] .Region	„eu-central-1“
Konfigurationselement „Konfiguration“	Ressourcen [i] .Details	
	SchemaVersion	„2018-10-08“
	Schweregrad. Bezeichnung	Weitere Informationen finden Sie weiter unten unter „Interpretation des Schweregrads“

Findetyp für die Auswertung der Konfigurationsregel	ASFF-Ergebnistyp	Hartcodierter Wert
	Typen	["Software- und Konfigurationsprüfungen"]
Detail. newEvaluationResult. Art der Konformität	Konformität. Status	„FEHLGESCHLAGEN“, „NOT_AVAILABLE“, „BESTANDEN“ oder „WARNUNG“
	Arbeitsablauf.Status	„RESOLVED“, wenn ein AWS Config Ergebnis mit dem Wert Compliance.Status auf „PASSED“ generiert wird oder wenn sich der Wert Compliance.Status von „FAILED“ auf „PASSED“ ändert. Andernfalls lautet Workflow.Status „NEW“. Sie können diesen Wert mit der BatchUpdateFindings API-Operation ändern.

Interpretation der Bezeichnung des Schweregrads

Für alle Ergebnisse aus AWS Config Regelauswertungen ist in der ASFF standardmäßig der Schweregrad MITTEL angegeben. Sie können den Schweregrad eines Ergebnisses mit dem [BatchUpdateFindings](#)API-Vorgang aktualisieren.

Typischer Befund von AWS Config

Security Hub CSPM wandelt AWS Config Regelauswertungen in Ergebnisse um, die dem ASFF folgen. Im Folgenden finden Sie ein Beispiel für ein typisches Ergebnis aus AWS Config der ASFF.

Note

Wenn die Beschreibung mehr als 1.024 Zeichen umfasst, wird sie auf 1.024 Zeichen gekürzt und am Ende steht „(gekürzt)“.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/finding/45g070df80cb50b68fa6a43594kc6fda1e517932",
  "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/config",
  "ProductName": "Config",
  "CompanyName": "AWS",
  "Region": "eu-central-1",
  "GeneratorId": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks"
  ],
  "CreatedAt": "2022-04-15T05:00:37.181Z",
  "UpdatedAt": "2022-04-19T21:20:15.056Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": 40
  },
  "Title": "s3-bucket-level-public-access-prohibited-config-integration-demo",
  "Description": "This finding is created for a resource compliance change for config rule: s3-bucket-level-public-access-prohibited-config-integration-demo",
  "ProductFields": {
    "aws/securityhub/ProductName": "Config",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/config/arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/finding/46f070df80cd50b68fa6a43594dc5fda1e517902",
    "aws/config/ConfigRuleArn": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq",
    "aws/config/ConfigRuleName": "s3-bucket-level-public-access-prohibited-config-integration-demo",
    "aws/config/ConfigComplianceType": "NON_COMPLIANT"
  },
  "Resources": [{
    "Type": "AwsS3Bucket",
    "Id": "arn:aws:s3:::amzn-s3-demo-bucket",
    "Partition": "aws",
    "Region": "eu-central-1",
    "Details": {
      "AwsS3Bucket": {
        "OwnerId": "4edbbba300f1caa608fba2aad2c8fcfe30c32ca32777f64451eec4fb2a0f10d8c",
```

```
    "CreatedAt": "2022-04-15T04:32:53.000Z"
  }
}
]],
"Compliance": {
  "Status": "FAILED"
},
"WorkflowState": "NEW",
"Workflow": {
  "Status": "NEW"
},
"RecordState": "ACTIVE",
"FindingProviderFields": {
  "Severity": {
    "Label": "MEDIUM"
  },
  "Types": [
    "Software and Configuration Checks"
  ]
}
}
```

Aktivieren und Konfigurieren der Integration

Nachdem Sie Security Hub CSPM aktiviert haben, wird diese Integration automatisch aktiviert. AWS Config beginnt sofort, Ergebnisse an Security Hub CSPM zu senden.

Einstellung der Veröffentlichung der Ergebnisse im Security Hub CSPM

Um das Senden von Ergebnissen an Security Hub CSPM zu beenden, können Sie die Security Hub CSPM-Konsole oder die Security Hub CSPM-API verwenden.

Anweisungen zum Stoppen des Flusses von Ergebnissen finden Sie unter [Den Fluss von Erkenntnissen aus einer Security Hub CSPM-Integration ermöglichen](#)

AWS Firewall Manager (Sendet Ergebnisse)

Firewall Manager sendet Ergebnisse an Security Hub CSPM, wenn eine Web Application Firewall (WAF) -Richtlinie für Ressourcen oder eine Web Access Control List (Web ACL) -Regel nicht den Vorschriften entspricht. Firewall Manager sendet auch Erkenntnisse, wenn AWS Shield Advanced Ressourcen nicht geschützt sind oder wenn ein Angriff erkannt wird.

Nachdem Sie Security Hub CSPM aktiviert haben, wird diese Integration automatisch aktiviert. Firewall Manager beginnt sofort, Ergebnisse an Security Hub CSPM zu senden.

Weitere Informationen zur Integration finden Sie auf der Seite Integrationen in der Security Hub CSPM-Konsole.

Weitere Informationen zu Firewall Manager finden Sie im [AWS WAF Entwicklerhandbuch](#).

Amazon GuardDuty (Sendet Ergebnisse)

GuardDuty sendet alle von ihm generierten Befundtypen an Security Hub CSPM. Für einige Befundtypen gelten Voraussetzungen, Aktivierungsanforderungen oder regionale Einschränkungen. Weitere Informationen [GuardDuty finden Sie im GuardDuty Amazon-Benutzerhandbuch unter Typen suchen](#).

Neue Ergebnisse von GuardDuty werden innerhalb von fünf Minuten an Security Hub CSPM gesendet. Aktualisierungen der Ergebnisse werden auf der Grundlage der Einstellung Aktualisierte Ergebnisse für Amazon EventBridge in den GuardDuty Einstellungen gesendet.

Wenn Sie GuardDuty Stichprobenergebnisse mithilfe der GuardDuty Einstellungsseite generieren, empfängt Security Hub CSPM die Probenergebnisse und lässt das Präfix [Sample] im Befundtyp weg. Beispielsweise GuardDuty [SAMPLE] Recon:IAMUser/ResourcePermissions wird der Suchtyp der Stichprobe in wie Recon:IAMUser/ResourcePermissions in Security Hub CSPM angezeigt.

Nachdem Sie Security Hub CSPM aktiviert haben, wird diese Integration automatisch aktiviert. GuardDuty beginnt sofort, Ergebnisse an Security Hub CSPM zu senden.

Weitere Informationen zur GuardDuty Integration finden Sie unter [Integration mit AWS Security Hub Cloud Security Posture Management \(CSPM\)](#) im GuardDuty Amazon-Benutzerhandbuch.

AWS Health (Sendet Ergebnisse)

AWS Health bietet fortlaufenden Einblick in die Leistung Ihrer Ressourcen und die Verfügbarkeit Ihrer AWS-Services Ressourcen AWS-Konten. Sie können AWS Health Ereignisse verwenden, um zu erfahren, wie sich Änderungen an Diensten und Ressourcen auf Ihre Anwendungen auswirken können, die auf ausgeführt AWS werden.

Die Integration mit verwendet AWS Health nichtBatchImportFindings. AWS Health Verwendet stattdessen service-to-service Ereignisnachrichten, um Ergebnisse an Security Hub CSPM zu senden.

Weitere Informationen zur Integration finden Sie in den folgenden Abschnitten.

Wie AWS Health sendet man Ergebnisse an Security Hub CSPM

In Security Hub CSPM werden Sicherheitsprobleme als Ergebnisse verfolgt. Einige Ergebnisse stammen aus Problemen, die von anderen AWS Diensten oder von Drittanbietern entdeckt wurden. Security Hub CSPM verfügt außerdem über eine Reihe von Regeln, anhand derer Sicherheitsprobleme erkannt und Ergebnisse generiert werden.

Security Hub CSPM bietet Tools zur Verwaltung von Ergebnissen aus all diesen Quellen. Sie können Listen mit Erkenntnissen anzeigen und filtern und Details zu einer Erkenntnis anzeigen. Siehe [Überprüfung der Funddetails und des Verlaufs in Security Hub CSPM](#). Sie können auch den Status einer Untersuchung zu einer Erkenntnis nachverfolgen. Siehe [Den Workflow-Status von Ergebnissen in Security Hub CSPM festlegen](#).

Alle Ergebnisse in Security Hub CSPM verwenden ein Standard-JSON-Format namens [AWS Format für Sicherheitssuche \(ASFF\)](#). ASFF enthält Einzelheiten zur Ursache des Problems, zu den betroffenen Ressourcen und zum aktuellen Stand der Ergebnisse.

AWS Health ist einer der AWS Dienste, der Ergebnisse an Security Hub CSPM sendet.

Arten von Ergebnissen, die AWS Health an Security Hub CSPM gesendet werden

AWS Health Sendet nach der Aktivierung der Integration Ergebnisse, die eine oder mehrere der aufgelisteten Spezifikationen erfüllen, an Security Hub CSPM. Security Hub CSPM nimmt die Ergebnisse in die auf. [AWS Format für Sicherheitssuche \(ASFF\)](#)

- Ergebnisse, die einen der folgenden Werte enthalten für: AWS-Service
 - RISK
 - ABUSE
 - ACM
 - CLOUDHSM
 - CLOUDTRAIL
 - CONFIG
 - CONTROLTOWER
 - DETECTIVE
 - EVENTS
 - GUARDDUTY

- IAM
 - INSPECTOR
 - KMS
 - MACIE
 - SES
 - SECURITYHUB
 - SHIELD
 - SSO
 - COGNITO
 - IOTDEVICEDEFENDER
 - NETWORKFIREWALL
 - ROUTE53
 - WAF
 - FIREWALLMANAGER
 - SECRETSMANAGER
 - BACKUP
 - AUDITMANAGER
 - ARTIFACT
 - CLOUDENDURE
 - CODEGURU
 - ORGANIZATIONS
 - DIRECTORYSERVICE
 - RESOURCEMANAGER
 - CLOUDWATCH
 - DRS
 - INSPECTOR2
 - RESILIENCEHUB
- Ergebnisse mit den Wörtern securityabuse, oder certificate im AWS Health typeCode Feld

AWS Health Ergebnisse an Security Hub CSPM senden

Wenn Sie sich dafür entscheiden, Ergebnisse von zu akzeptieren AWS Health, weist Security Hub CSPM automatisch die Berechtigungen zu, die für den Empfang der Ergebnisse von erforderlich sind. AWS Health Security Hub CSPM verwendet service-to-service Level-Berechtigungen, die Ihnen eine sichere und einfache Möglichkeit bieten, diese Integration zu aktivieren und Ergebnisse in Ihrem Namen AWS Health über EventBridge Amazon zu importieren. Wenn Sie „Ergebnisse akzeptieren“ wählen, erteilt Security Hub CSPM die Erlaubnis, Ergebnisse von zu verwenden. AWS Health

Latenz für das Senden von Erkenntnissen

Wenn ein neues Ergebnis AWS Health erstellt wird, wird es normalerweise innerhalb von fünf Minuten an Security Hub CSPM gesendet.

Wiederholter Versuch, wenn Security Hub CSPM nicht verfügbar ist

AWS Health sendet die Ergebnisse nach bestem Wissen und Gewissen an Security Hub CSPM. EventBridge Wenn ein Ereignis nicht erfolgreich an Security Hub CSPM übermittelt wurde, wird EventBridge erneut versucht, das Ereignis für 24 Stunden zu senden.

Aktualisierung vorhandener Ergebnisse in Security Hub CSPM

Nachdem ein Ergebnis an Security Hub CSPM AWS Health gesendet wurde, kann es Updates zu demselben Ergebnis senden, um zusätzliche Beobachtungen der Findungsaktivität an Security Hub CSPM widerzuspiegeln.

Regionen, in denen Ergebnisse vorliegen

AWS Health Sendet bei globalen Ereignissen Ergebnisse an Security Hub CSPM in us-east-1 (AWS Partition), cn-northwest-1 (Partition China) und -1 (Partition). gov-us-west GovCloud AWS Health sendet regionsspezifische Ereignisse an Security Hub CSPM in derselben Region oder Regionen, in denen die Ereignisse auftreten.

AWS Health Ergebnisse in Security Hub CSPM anzeigen

Um Ihre AWS Health Ergebnisse in Security Hub CSPM anzuzeigen, wählen Sie im Navigationsbereich Findings aus. Um die Ergebnisse so zu filtern, dass nur AWS Health Ergebnisse angezeigt werden, wählen Sie Health aus dem Feld Produktname aus.

Interpretieren AWS Health von gefundenen Namen in Security Hub CSPM

AWS Health sendet die Ergebnisse mit dem an Security Hub CSPM. [AWS Format für Sicherheitssuche \(ASFF\)](#) AWS Health Die Suche verwendet ein anderes Ereignismuster als das

Security Hub CSPM ASFF-Format. In der folgenden Tabelle sind alle Ergebnisfelder mit ihren ASFF-Gegenständen aufgeführt, so wie sie in Security Hub CSPM erscheinen. AWS Health

Art Health Gesundheitsbefundung	ASFF-Ergebnistyp	Hartcodierter Wert
Konto	AwsAccountId	
Detail.StartTime	CreatedAt	
Detail.EventDescription.Letzte Beschreibung	Beschreibung	
Detail. eventTypeCode	GeneratorId	
detail.eventArn (einschließlich Konto) + Hash von detail.StartTime	Id	
<region>„arn:aws:securityhub::“ product/aws/health	ProductArn	
Konto oder resourceId	Ressourcen [i] .id	
	Ressourcen [i] .Type	„Andere“
	SchemaVersion	„2018-10-08“
	Schweregrad. Bezeichnung	Weitere Informationen finden Sie weiter unten unter „Interpretation des Schweregrads“
Detail „AWS Health -“. eventTypeCode	Title	
-	Typen	[„Software- und Konfigurationschecks“]
event.time	UpdatedAt	

Art Health Gesundheitsbefundung	ASFF-Ergebnistyp	Hartcodierter Wert
URL des Ereignisses auf der Health Console	SourceUrl	

Der Schweregrad wird interpretiert

Der Schweregrad im ASFF-Ergebnis wird anhand der folgenden Logik bestimmt:

- Schweregrad KRITISCH wenn:
 - Das service Feld im AWS Health Ergebnis hat den Wert Risk
 - Das typeCode Feld im AWS Health Befund hat den Wert AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION
 - Das typeCode Feld im AWS Health Befund hat den Wert AWS_SHIELD_INTERNET_TRAFFIC_LIMITATIONS_PLACED_IN_RESPONSE_TO_DDOS_ATTACK
 - Das typeCode Feld im AWS Health Befund hat den Wert AWS_SHIELD_IS_RESPONDING_TO_A_DDOS_ATTACK_AGAINST_YOUR_AWS_RESOURCES

Schweregrad HOCH, wenn:

- Das service Feld im AWS Health Ergebnis hat den Wert Abuse
- Das typeCode Feld im AWS Health Befund enthält den Wert SECURITY_NOTIFICATION
- Das typeCode Feld im AWS Health Befund enthält den Wert ABUSE_DETECTION

Schweregrad MITTEL, wenn:

- Das service Feld im Ergebnis ist eines der folgenden: ACM,,,,,,ARTIFACT,,AUDITMANAGER,BACKUP,CLOUDENDURE,CLOUDHSM,,CLOUDTRAIL,CLOUDWATCH oder WAF
- Das TypeCode-Feld im AWS Health Ergebnis enthält den Wert CERTIFICATE
- Das TypeCode-Feld im AWS Health Befund enthält den Wert END_OF_SUPPORT

Typischer Befund von AWS Health

AWS Health sendet Ergebnisse mit dem an Security Hub CSPM. [AWS Format für Sicherheitssuche](#)

[\(ASFF\)](#) Im Folgenden finden Sie ein Beispiel für ein typisches Ergebnis von AWS Health

AWS Dienste, die Ergebnisse an Security Hub CSPM senden

Note

Wenn die Beschreibung mehr als 1024 Zeichen umfasst, wird sie auf 1024 Zeichen gekürzt und am Ende steht (gekürzt).

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:health:us-east-1:123456789012:event/SES/
AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-
b533-78e29f49de96/101F7FBAEFC663977DA09CFF56A29236602834D2D361E6A8CA5140BFB3A69B30",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/health",
  "GeneratorId": "AWS_SES_CMF_PENDING_TO_SUCCESS",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks"
  ],
  "CreatedAt": "2022-01-07T16:34:04.000Z",
  "UpdatedAt": "2022-01-07T19:17:43.000Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": 40
  },
  "Title": "AWS Health - AWS_SES_CMF_PENDING_TO_SUCCESS",
  "Description": "Congratulations! Amazon SES has successfully detected the
MX record required to use 4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com as a custom MAIL FROM domain for verified identity cmf.pinpoint.sysmon-
iad.adzel.com in AWS Region US East (N. Virginia).\\n\\nYou can now use this MAIL
FROM domain with cmf.pinpoint.sysmon-iad.adzel.com and any other verified identity
that is configured to use it. For information about how to configure a verified
identity to use a custom MAIL FROM domain, see http://docs.aws.amazon.com/ses/latest/
DeveloperGuide/mail-from-set.html .\\n\\nPlease note that this email only applies to
AWS Region US East (N. Virginia).",
  "SourceUrl": "https://phd.aws.amazon.com/phd/home#/event-log?
eventID=arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
  "ProductFields": {
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/
aws/health/arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
    "aws/securityhub/ProductName": "Health",
```

```

        "aws/securityhub/CompanyName": "AWS"
    },
    "Resources": [
        {
            "Type": "Other",
            "Id": "4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com"
        }
    ],
    "WorkflowState": "NEW",
    "Workflow": {
        "Status": "NEW"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
        "Severity": {
            "Label": "MEDIUM"
        },
        "Types": [
            "Software and Configuration Checks"
        ]
    }
}
]
}

```

Aktivieren und Konfigurieren der Integration

Nachdem Sie Security Hub CSPM aktiviert haben, wird diese Integration automatisch aktiviert. AWS Health beginnt sofort, Ergebnisse an Security Hub CSPM zu senden.

Einstellung der Veröffentlichung der Ergebnisse im Security Hub CSPM

Um das Senden von Ergebnissen an Security Hub CSPM zu beenden, können Sie die Security Hub CSPM-Konsole oder die Security Hub CSPM-API verwenden.

Anweisungen zum Stoppen des Flusses von Ergebnissen finden Sie unter [Den Fluss von Erkenntnissen aus einer Security Hub CSPM-Integration ermöglichen](#)

AWS Identity and Access Management Access Analyzer (Sendet Ergebnisse)

Mit IAM Access Analyzer werden alle Ergebnisse an Security Hub CSPM gesendet.

IAM Access Analyzer analysiert anhand von logischer Argumentation ressourcenbasierte Richtlinien, die auf unterstützte Ressourcen in Ihrem Konto angewendet werden. IAM Access Analyzer generiert ein Ergebnis, wenn er eine Richtlinienaussage entdeckt, die einem externen Principal den Zugriff auf eine Ressource in Ihrem Konto ermöglicht.

In IAM Access Analyzer kann nur das Administratorkonto Ergebnisse für Analyzer sehen, die für eine Organisation gelten. Bei Organisationsanalyseprogrammen gibt das `AwsAccountId` ASFF-Feld die Administratorkonto-ID an. Das `ResourceOwnerAccount` Feld `ProductFields` darunter gibt das Konto an, in dem das Ergebnis entdeckt wurde. Wenn Sie Analyzer für jedes Konto einzeln aktivieren, generiert Security Hub CSPM mehrere Ergebnisse, eines, das die Administratorkonto-ID identifiziert, und eines, das die Ressourcenkonto-ID identifiziert.

Weitere Informationen finden Sie unter [Integration mit AWS Security Hub Cloud Security Posture Management \(CSPM\)](#) im IAM-Benutzerhandbuch.

Amazon Inspector (Sendet Ergebnisse)

Amazon Inspector ist ein Schwachstellen-Management-Service, der Ihre AWS Workloads kontinuierlich auf Schwachstellen überprüft. Amazon Inspector erkennt und scannt automatisch EC2 Amazon-Instances und Container-Images, die sich in der Amazon Elastic Container Registry befinden. Der Scan sucht nach Sicherheitslücken in Software und unbeabsichtigter Netzwerkgefährdung.

Nachdem Sie Security Hub CSPM aktiviert haben, wird diese Integration automatisch aktiviert. Amazon Inspector beginnt sofort, alle Ergebnisse, die es generiert, an Security Hub CSPM zu senden.

Weitere Informationen zur Integration finden Sie unter [Integration mit AWS Security Hub Cloud Security Posture Management \(CSPM\)](#) im Amazon Inspector Inspector-Benutzerhandbuch.

Security Hub CSPM kann auch Ergebnisse von Amazon Inspector Classic erhalten. Amazon Inspector Classic sendet Ergebnisse an Security Hub CSPM, die im Rahmen von Bewertungsläufen für alle unterstützten Regelpakete generiert wurden.

Weitere Informationen zur Integration finden Sie unter [Integration mit AWS Security Hub Cloud Security Posture Management \(CSPM\)](#) im Amazon Inspector Classic-Benutzerhandbuch.

Die Ergebnisse für Amazon Inspector und Amazon Inspector Classic verwenden denselben Produkt-ARN. Die Ergebnisse von Amazon Inspector haben den folgenden Eintrag in `ProductFields`:

```
"aws/inspector/ProductVersion": "2",
```

Note

Von [Amazon Inspector Code Security generierte Sicherheitsergebnisse](#) sind für diese Integration nicht verfügbar. Sie können jedoch in der Amazon Inspector-Konsole und über die Amazon [Inspector-API](#) auf diese speziellen Ergebnisse zugreifen.

AWS IoT Device Defender (Sendet Ergebnisse)

AWS IoT Device Defender ist ein Sicherheitsdienst, der die Konfiguration Ihrer IoT-Geräte überprüft, angeschlossene Geräte überwacht, um ungewöhnliches Verhalten zu erkennen, und zur Minderung von Sicherheitsrisiken beiträgt.

Nachdem Sie AWS IoT Device Defender sowohl als auch Security Hub CSPM aktiviert haben, rufen Sie die [Integrationsseite der Security Hub CSPM-Konsole](#) auf und wählen Sie Ergebnisse akzeptieren für Audit, Detect oder beides aus. AWS IoT Device Defender Audit and Detect beginnt, alle Ergebnisse an Security Hub CSPM zu senden.

AWS IoT Device Defender Audit sendet Prüfungszusammenfassungen an Security Hub CSPM, die allgemeine Informationen für einen bestimmten Prüfungstyp und eine bestimmte Prüfungsaufgabe enthalten. AWS IoT Device Defender Detect sendet festgestellte Verstöße für maschinelles Lernen (ML), statistisches und statisches Verhalten an Security Hub CSPM. Audit sendet auch gefundene Updates an Security Hub CSPM.

Weitere Informationen zu dieser Integration finden Sie unter [Integration mit AWS Security Hub Cloud Security Posture Management \(CSPM\)](#) im AWS IoT Entwicklerhandbuch.

Amazon Macie (Sendet Ergebnisse)

Amazon Macie ist ein Datensicherheitsservice, der sensible Daten mithilfe von Machine Learning und Musterabgleich entdeckt, Einblicke in Datensicherheitsrisiken bietet und automatischen Schutz vor diesen Risiken ermöglicht. Ein Ergebnis von Macie kann darauf hinweisen, dass in Ihrem Amazon S3 S3-Datenbestand ein potenzieller Richtlinienverstoß vorliegt oder sensible Daten vorhanden sind.

Nachdem Sie Security Hub CSPM aktiviert haben, beginnt Macie automatisch, Richtlinienenergebnisse an Security Hub CSPM zu senden. Sie können die Integration so konfigurieren, dass auch Ergebnisse vertraulicher Daten an Security Hub CSPM gesendet werden.

In Security Hub CSPM wird der Suchtyp für eine Richtlinie oder einen Fund vertraulicher Daten auf einen Wert geändert, der mit ASFF kompatibel ist. Beispielsweise wird der Policy:IAMUser/S3BucketPublic Findungstyp in Macie wie Effects/Data Exposure/Policy:IAMUser-S3BucketPublic in Security Hub CSPM angezeigt.

Macie sendet auch generierte Probenergebnisse an Security Hub CSPM. Bei Stichprobenergebnissen lautet der Name der betroffenen Ressource `macie-sample-finding-bucket` und der Wert für das `Sample` Feld lautet `true`.

Weitere Informationen finden Sie unter [Evaluierung der Macie-Ergebnisse mit Security Hub](#) im Amazon Macie Macie-Benutzerhandbuch.

Amazon Route 53 Resolver DNS-Firewall (Sendet Ergebnisse)

Mit der Amazon Route 53 Resolver DNS-Firewall können Sie ausgehenden DNS-Verkehr für Ihre Virtual Private Cloud (VPC) filtern und regulieren. Dazu erstellen Sie wiederverwendbare Sammlungen von Filterregeln in DNS-Firewall-Regelgruppen, verknüpfen die Regelgruppen mit Ihrer VPC und überwachen dann die Aktivitäten in DNS-Firewallprotokollen und -Metriken. Basierend auf der Aktivität können Sie das Verhalten der DNS-Firewall anpassen. Die DNS-Firewall ist eine Funktion von Route 53 Resolver.

Die Route 53 Resolver DNS Firewall kann verschiedene Arten von Ergebnissen an Security Hub CSPM senden:

- Ergebnisse im Zusammenhang mit Abfragen, bei denen es sich um blockierte oder Warnmeldungen für Domänen handelt, die AWS verwalteten Domänenlisten zugeordnet sind. AWS
- Ergebnisse im Zusammenhang mit Anfragen, die blockiert wurden oder bei denen eine Warnung ausgelöst wurde, für Domänen, die mit einer von Ihnen definierten, benutzerdefinierten Domänenliste verknüpft sind.
- Ergebnisse im Zusammenhang mit Abfragen, die von DNS Firewall Advanced blockiert wurden oder bei denen eine Warnung angezeigt wurde. Dabei handelt es sich um eine Route 53-Resolver-Funktion, mit der Abfragen im Zusammenhang mit komplexen DNS-Bedrohungen wie Algorithmen zur Domänengenerierung (DGAs) und DNS-Tunneling erkannt werden können.

Nachdem Sie Security Hub CSPM und Route 53 Resolver DNS Firewall aktiviert haben, beginnt die DNS-Firewall automatisch, Ergebnisse für AWS verwaltete Domänenlisten und DNS Firewall Advanced an Security Hub CSPM zu senden. Um auch Ergebnisse für eine benutzerdefinierte

Domainliste an Security Hub CSPM zu senden, aktivieren Sie die Integration in Security Hub CSPM manuell.

In Security Hub CSPM haben alle Ergebnisse der Route 53 Resolver DNS Firewall den folgenden Typ: `TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation`

Weitere Informationen finden Sie unter [Senden von Ergebnissen von der Route 53 Resolver DNS Firewall an Security Hub](#) im Amazon Route 53-Entwicklerhandbuch.

AWS Systems Manager Patch Manager (Sendet Ergebnisse)

AWS Systems Manager Patch Manager sendet Ergebnisse an Security Hub CSPM, wenn Instances in der Flotte eines Kunden nicht mehr dem Patch-Compliance-Standard entsprechen.

Patch Manager automatisiert das Patchen verwalteter Instances mit sicherheitsrelevanten und anderen Arten von Updates.

Nachdem Sie Security Hub CSPM aktiviert haben, wird diese Integration automatisch aktiviert. Systems Manager Patch Manager beginnt sofort, Ergebnisse an Security Hub CSPM zu senden.

Weitere Informationen zur Verwendung von Patch Manager finden Sie unter [AWS Systems Manager Patch Manager](#) im AWS Systems Manager Benutzerhandbuch.

AWS Dienste, die Erkenntnisse von Security Hub CSPM erhalten

Die folgenden AWS Dienste sind in Security Hub CSPM integriert und beziehen Ergebnisse von Security Hub CSPM. Sofern angegeben, kann der integrierte Dienst die Ergebnisse auch aktualisieren. In diesem Fall wird das Auffinden von Updates, die Sie im integrierten Dienst vornehmen, auch in Security Hub CSPM widergespiegelt.

AWS Audit Manager (Erhält Ergebnisse)

AWS Audit Manager erhält Ergebnisse von Security Hub CSPM. Diese Ergebnisse helfen den Benutzern von Audit Manager, sich auf Audits vorzubereiten.

Weitere Informationen zu Audit Manager finden Sie im [AWS Audit Manager Manager-Benutzerhandbuch](#). [AWS Security Hub Cloud Security Posture Management \(CSPM\) -Prüfungen, die von unterstützt werden](#), AWS Audit Manager listet die Kontrollen auf, für die Security Hub CSPM Ergebnisse an Audit Manager sendet.

Amazon Q Developer in Chat-Anwendungen (erhält Ergebnisse)

Amazon Q Developer in Chat-Anwendungen ist ein interaktiver Agent, der Ihnen hilft, Ihre AWS Ressourcen in Ihren Slack-Kanälen und Amazon Chime Chime-Chatrooms zu überwachen und mit ihnen zu interagieren.

Amazon Q Developer in Chat-Anwendungen erhält Ergebnisse von Security Hub CSPM.

Weitere Informationen zur Integration von Amazon Q Developer in Chat-Anwendungen mit Security Hub CSPM finden Sie in der [Übersicht über die Security Hub CSPM-Integration](#) im Administratorhandbuch für Amazon Q Developer in Chat-Anwendungen.

Amazon Detective (erhält Ergebnisse)

Detective sammelt automatisch Protokolldaten aus Ihren AWS Ressourcen und nutzt maschinelles Lernen, statistische Analysen und Graphentheorie, um Sie bei der Visualisierung und Durchführung schnellerer und effizienterer Sicherheitsuntersuchungen zu unterstützen.

Die Security Hub CSPM-Integration mit Detective ermöglicht es Ihnen, von GuardDuty Amazon-Ergebnissen in Security Hub CSPM zu Detective zu wechseln. Anschließend können Sie die Detective-Tools und Visualisierungen verwenden, um sie zu untersuchen. Die Integration erfordert keine zusätzliche Konfiguration in Security Hub CSPM oder Detective.

Für Ergebnisse, die von anderen stammen AWS-Services, enthält der Bereich mit den Ergebnisdetails auf der Security Hub CSPM-Konsole den Unterabschnitt Investigate in Detective. Dieser Unterabschnitt enthält einen Link zu Detective, über den Sie das Sicherheitsproblem, das durch den Befund gemeldet wurde, weiter untersuchen können. Sie können in Detective auch ein Verhaltensdiagramm erstellen, das auf den Ergebnissen des Security Hub CSPM basiert, um effektivere Untersuchungen durchzuführen. Weitere Informationen finden Sie in den [AWS Sicherheitsergebnissen](#) im Amazon Detective Administration Guide.

Wenn die regionsübergreifende Aggregation aktiviert ist und Sie von der Aggregationsregion aus wechseln, wird Detective in der Region geöffnet, aus der das Ergebnis stammt.

Wenn ein Link nicht funktioniert, finden Sie Hinweise zur Fehlerbehebung unter [Troubleshooting the Pivot](#).

Amazon Security Lake (erhält Ergebnisse)

Security Lake ist ein vollständig verwalteter Sicherheits-Data-Lake-Service. Sie können Security Lake verwenden, um Sicherheitsdaten aus Cloud-, lokalen und benutzerdefinierten Quellen automatisch in

einem Data Lake zu zentralisieren, der in Ihrem Konto gespeichert ist. Abonnenten können Daten aus Security Lake für Ermittlungs- und Analysezwecke nutzen.

Um diese Integration zu aktivieren, müssen Sie beide Dienste aktivieren und Security Hub CSPM als Quelle in der Security Lake-Konsole, der Security Lake-API oder hinzufügen. AWS CLI Sobald Sie diese Schritte abgeschlossen haben, beginnt Security Hub CSPM, alle Ergebnisse an Security Lake zu senden.

Security Lake normalisiert die CSPM-Ergebnisse von Security Hub automatisch und konvertiert sie in ein standardisiertes Open-Source-Schema namens Open Cybersecurity Schema Framework (OCSF). In Security Lake können Sie einen oder mehrere Abonnenten hinzufügen, um die CSPM-Ergebnisse von Security Hub zu nutzen.

Weitere Informationen zu dieser Integration, einschließlich Anweisungen zum Hinzufügen von Security Hub CSPM als Quelle und zum Erstellen von Abonnenten, finden Sie unter [Integration mit AWS Security Hub Cloud Security Posture Management \(CSPM\)](#) im Amazon Security Lake-Benutzerhandbuch.

AWS Systems Manager Explorer und OpsCenter (Empfängt und aktualisiert Ergebnisse)

AWS Systems Manager Erkunden und OpsCenter empfangen Sie Ergebnisse von Security Hub CSPM und aktualisieren Sie diese Ergebnisse in Security Hub CSPM.

Explorer bietet Ihnen ein anpassbares Dashboard, das wichtige Einblicke und Analysen zum Betriebsstatus und zur Leistung Ihrer Umgebung bietet. AWS

OpsCenter bietet Ihnen einen zentralen Ort, an dem Sie betriebliche Arbeitsaufgaben anzeigen, untersuchen und lösen können.

Weitere Informationen zu Explorer und OpsCenter finden Sie unter [Operations Management](#) im AWS Systems Manager Benutzerhandbuch.

AWS Trusted Advisor (Erhält Ergebnisse)

Trusted Advisor stützt sich auf bewährte Verfahren, die bei der Betreuung von Hunderttausenden von AWS Kunden gelernt wurden. Trusted Advisor untersucht Ihre AWS Umgebung und gibt dann Empfehlungen, wenn Möglichkeiten bestehen, Geld zu sparen, die Systemverfügbarkeit und -leistung zu verbessern oder Sicherheitslücken zu schließen.

Wenn Sie Trusted Advisor sowohl als auch Security Hub CSPM aktivieren, wird die Integration automatisch aktualisiert.

Security Hub CSPM sendet die Ergebnisse seiner AWS Foundational Security Best Practices-Prüfungen an Trusted Advisor

Weitere Informationen zur Security Hub CSPM-Integration mit Trusted Advisor finden Sie unter [Anzeigen von AWS Security Hub Cloud Security Posture Management \(CSPM\) -Steuerelementen AWS Trusted Advisor im AWS Support-Benutzerhandbuch](#).

Produktintegrationen von Drittanbietern mit Security Hub CSPM

AWS Security Hub Cloud Security Posture Management (CSPM) lässt sich in mehrere Produkte von Drittanbietern integrieren. Eine Integration kann eine oder mehrere der folgenden Aktionen ausführen:

- Senden Sie die generierten Ergebnisse an Security Hub CSPM
- Erhalten Sie Ergebnisse von Security Hub CSPM
- Ergebnisse im Security Hub CSPM aktualisieren

Integrationen, die Ergebnisse an Security Hub CSPM senden, haben einen Amazon-Ressourcennamen (ARN).

Eine Integration ist möglicherweise nicht in allen verfügbar. AWS-Regionen Wenn eine Integration in der Region, in der Sie derzeit angemeldet sind, auf der Security Hub CSPM-Konsole nicht unterstützt wird, wird sie nicht auf der Integrationsseite der Konsole angezeigt. Eine Liste der Integrationen, die in den Regionen China und verfügbar sind AWS GovCloud (US) Regions, finden Sie unter [Verfügbarkeit von Integrationen nach Regionen](#).

<Wenn Sie über eine Sicherheitslösung verfügen und daran interessiert sind, ein Weitere Informationen finden Sie im Leitfaden zur [Partnerintegration](#).

Überblick über Integrationen von Drittanbietern mit Security Hub CSPM

Die folgende Tabelle bietet einen Überblick über die Integrationen von Drittanbietern, die Ergebnisse an Security Hub CSPM senden oder Ergebnisse von Security Hub CSPM empfangen können.

Integration	Richtung	ARN (falls zutreffend)
3CORESec – 3CORESec NTA	Sendet Ergebnisse	arn:aws:securityhub: <REGION> ::product/3coresec/3coresec
Alert Logic – SIEMless Threat Management	Sendet Ergebnisse	arn:aws:securityhub: <REGION> :733251395267:product/alertlogic/althreatmanagement
Aqua Security – Aqua Cloud Native Security Platform	Sendet Ergebnisse	arn:aws:securityhub: <REGION> ::product/aquasecurity/aquasecurity
Aqua Security – Kube-bench	Sendet Ergebnisse	arn:aws:securityhub: <REGION> ::product/aqua-security/kube-bench
Armor – Armor Anywhere	Sendet Ergebnisse	arn:aws:securityhub: <REGION> :679703615338:product/armordefense/armoranywhere
AttackIQ – AttackIQ	Sendet Ergebnisse	arn:aws:securityhub: <REGION> ::product/attackiq/attackiq-platform
Barracuda Networks – Cloud Security Guardian	Sendet Ergebnisse	arn:aws:securityhub: <REGION> :151784055945:product/barracuda

Integration	Richtung	ARN (falls zutreffend)
		cuda/cloudsecurityguardian
BigID – BigID Enterprise	Sendet Ergebnisse	arn:aws:securityhub: <REGION>::product/bigid/bigid-enterprise
Blue Hexagon – Blue Hexagon forAWS	Sendet Ergebnisse	arn:aws:securityhub: <REGION>::product/blue-hexagon/blue-hexagon-for-aws
Check Point – CloudGuard IaaS	Sendet Ergebnisse	arn:aws:securityhub: <REGION>:758245563457:product/checkpoint/cloudguard-iaas
Check Point – CloudGuard Posture Management	Sendet Ergebnisse	arn:aws:securityhub: <REGION>:634729597623:product/checkpoint/dome9-arc
Claroty – xDome	Sendet Ergebnisse	arn:aws:securityhub: <REGION>::product/claroty/xdome
Cloud Storage Security—Antivirus for Amazon S3	Sendet Ergebnisse	arn:aws:securityhub: <REGION>::product/cloud-storage-security/antivirus-for-amazon-s3

Integration	Richtung	ARN (falls zutreffend)
Contrast Security	Sendet Ergebnisse	arn:aws:securityhub:<REGION>::product/contrast-security/security-assess
CrowdStrike – CrowdStrike Falcon	Sendet Ergebnisse	arn:aws:securityhub:<REGION>:517716713836:product/crowdstrike/crowdstrike-falcon
CyberArk – Privileged Threat Analytics	Sendet Ergebnisse	arn:aws:securityhub:<REGION>:749430749651:product/cyberark/cyberark-pta
Data Theorem – Data Theorem	Sendet Ergebnisse	arn:aws:securityhub:<REGION>::product/data-theorem/api-cloud-web-secure
Drata	Sendet Ergebnisse	arn:aws:securityhub:<REGION>::product/drata/drata-integration
Forcepoint – Forcepoint CASB	Sendet Ergebnisse	arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-casb

Integration	Richtung	ARN (falls zutreffend)
Forcepoint – Forcepoint Cloud Security Gateway	Sendet Ergebnisse	arn:aws:securityhub:<REGION>::product/forcepoint/forcepoint-cloud-security-gateway
Forcepoint – Forcepoint DLP	Sendet Ergebnisse	arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-dlp
Forcepoint – Forcepoint NGFW	Sendet Ergebnisse	arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-ngfw
Fugue – Fugue	Sendet Ergebnisse	arn:aws:securityhub:<REGION>::product/fugue/fugue
Guardicore – Centra 4.0	Sendet Ergebnisse	arn:aws:securityhub:<REGION>::product/guardicore/guardicore
HackerOne – Vulnerability Intelligence	Sendet Ergebnisse	arn:aws:securityhub:<REGION>::product/hackerone/vulnerability-intelligence
JFrog – Xray	Sendet Ergebnisse	arn:aws:securityhub:<REGION>::product/jfrog/jfrog-xray

Integration	Richtung	ARN (falls zutreffend)
Juniper Networks – vSRX Next Generation Firewall	Sendet Ergebnisse	arn:aws:securityhub:<REGION>::product/juniper-networks/vsrx-next-generation-firewall
k9 Security – Access Analyzer	Sendet Ergebnisse	arn:aws:securityhub:<REGION>::product/k9-security/access-analyzer
Lacework – Lacework	Sendet Ergebnisse	arn:aws:securityhub:<REGION>::product/lacework/lacework
McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)	Sendet Ergebnisse	arn:aws:securityhub:<REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws
NETSCOUT – NETSCOUT Cyber Investigator	Sendet Ergebnisse	arn:aws:securityhub:us-east-1::product/netscout/netscout-cyber-investigator
Palo Alto Networks – Prisma Cloud Compute	Sendet Ergebnisse	arn:aws:securityhub:<REGION>:496947949261:product/twistlock/twistlock-enterprise

Integration	Richtung	ARN (falls zutreffend)
Palo Alto Networks – Prisma Cloud Enterprise	Sendet Ergebnisse	arn:aws:securityhub: <REGION>:188619942792:product/paloaltonetworks/redlock
Plerion – Cloud Security Platform	Sendet Ergebnisse	arn:aws:securityhub: <REGION>::product/plerion/cloud-security-platform
Prowler – Prowler	Sendet Ergebnisse	arn:aws:securityhub: <REGION>::product/prowler/prowler
Qualys – Vulnerability Management	Sendet Ergebnisse	arn:aws:securityhub: <REGION>:805950163170:product/qualys/qualys-vm
Rapid7 – InsightVM	Sendet Ergebnisse	arn:aws:securityhub: <REGION>:336818582268:product/rapid7/insightvm
SecureCloudDB – SecureCloudDB	Sendet Ergebnisse	arn:aws:securityhub: <REGION>::product/secureclouddb/secureclouddb
SentinelOne – SentinelOne	Sendet Ergebnisse	arn:aws:securityhub: <REGION>::product/sentinelone/endpoint-protection

Integration	Richtung	ARN (falls zutreffend)
Snyk	Sendet Ergebnisse	arn:aws:securityhub: <region>::product/snyk/snyk
Sonrai Security – Sonrai Dig	Sendet Ergebnisse	arn:aws:securityhub: <REGION>::product/sonrai-security/sonrai-dig
Sophos – Server Protection	Sendet Ergebnisse	arn:aws:securityhub: <REGION>:062897671886:product/sophos/sophos-server-protection
StackRox – StackRox Kubernetes Security	Sendet Ergebnisse	arn:aws:securityhub: <REGION>::product/stackrox/kubernetes-security
Sumo Logic – Machine Data Analytics	Sendet Ergebnisse	arn:aws:securityhub: <REGION>:956882708938:product/sumologicinc/sumologic-mda
Symantec – Cloud Workload Protection	Sendet Ergebnisse	arn:aws:securityhub: <REGION>:754237914691:product/symantec-corp/symantec-cwp
Tenable – Tenable.io	Sendet Ergebnisse	arn:aws:securityhub: <REGION>:422820575223:product/tenable/tenable-io

Integration	Richtung	ARN (falls zutreffend)
Trend Micro – Cloud One	Sendet Ergebnisse	arn:aws:securityhub:<REGION>::product/trend-micro/cloud-one
Vectra – Cognito Detect	Sendet Ergebnisse	arn:aws:securityhub:<REGION>:978576646331:product/vectra-ai/cognito-detect
Wiz	Sendet Ergebnisse	arn:aws:securityhub:<REGION>::product/wiz-security/wiz-security
Atlassian - Jira Service Management	Empfängt und aktualisiert Ergebnisse	Nicht zutreffend
Atlassian - Jira Service Management Cloud	Empfängt und aktualisiert Ergebnisse	Nicht zutreffend
Atlassian – Opsgenie	Erhält Ergebnisse	Nicht zutreffend
Dynatrace	Erhält Ergebnisse	Nicht zutreffend
Fortinet – FortiCNP	Erhält Ergebnisse	Nicht zutreffend
IBM – QRadar	Erhält Ergebnisse	Nicht zutreffend
Logz.io Cloud SIEM	Erhält Ergebnisse	Nicht zutreffend
MetricStream	Erhält Ergebnisse	Nicht zutreffend
MicroFocus – MicroFocus Arcsight	Erhält Ergebnisse	Nicht zutreffend
New Relic Vulnerability Management	Erhält Ergebnisse	Nicht zutreffend

Integration	Richtung	ARN (falls zutreffend)
PagerDuty – PagerDuty	Erhält Ergebnisse	Nicht zutreffend
Palo Alto Networks – Cortex XSOAR	Erhält Ergebnisse	Nicht zutreffend
Palo Alto Networks – VM-Series	Erhält Ergebnisse	Nicht zutreffend
Rackspace Technology – Cloud Native Security	Erhält Ergebnisse	Nicht zutreffend
Rapid7 – InsightConnect	Erhält Ergebnisse	Nicht zutreffend
RSA – RSA Archer	Erhält Ergebnisse	Nicht zutreffend
ServiceNow – ITSM	Empfängt und aktualisiert Ergebnisse	Nicht zutreffend
Slack – Slack	Erhält Ergebnisse	Nicht zutreffend
Splunk – Splunk Enterprise	Erhält Ergebnisse	Nicht zutreffend
Splunk – Splunk Phantom	Erhält Ergebnisse	Nicht zutreffend
ThreatModeler	Erhält Ergebnisse	Nicht zutreffend
Trellix – Trellix Helix	Erhält Ergebnisse	Nicht zutreffend
Caveonix – Caveonix Cloud	Sendet und empfängt Ergebnisse	arn:aws:securityhub:<REGION>::product/caveonix/caveonix-cloud
Cloud Custodian – Cloud Custodian	Sendet und empfängt Ergebnisse	arn:aws:securityhub:<REGION>::product/cloud-custodian/cloud-custodian

Integration	Richtung	ARN (falls zutreffend)
DisruptOps, Inc. – DisruptOPS	Sendet und empfängt Ergebnisse	arn:aws:securityhub:<REGION>::product/disruptops-inc/disruptops
Kion	Sendet und empfängt Ergebnisse	arn:aws:securityhub:<REGION>::product/cloudtamerio/cloudtamerio
Turbot – Turbot	Sendet und empfängt Ergebnisse	arn:aws:securityhub:<REGION>:453761072151:product/turbot/turbot

Integrationen von Drittanbietern, die Ergebnisse an Security Hub CSPM senden

Die folgenden Produktintegrationen von Drittanbietern können Ergebnisse an Security Hub CSPM senden. Security Hub CSPM wandelt die Ergebnisse in das [AWS Security](#) Finding Format um.

3CORESec – 3CORESec NTA

Integrationstyp: Senden

Produkt-ARN: arn:aws:securityhub:<REGION>::product/3coresec/3coresec

3CORESec bietet verwaltete Erkennungsdienste sowohl für lokale Umgebungen als auch für AWS Systeme. Ihre Integration mit Security Hub CSPM ermöglicht Einblicke in Bedrohungen wie Malware, Rechteauserweiterung, laterale Bewegungen und unsachgemäße Netzwerksegmentierung.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Alert Logic – SIEMless Threat Management

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:733251395267:product/alertlogic/althreatmanagement`

Sorgen Sie für das richtige Maß an Schutz: Sichtbarkeit von Schwachstellen und Ressourcen, Bedrohungserkennung und Vorfallmanagement sowie zugewiesene SOC-Analystenoptionen. AWS WAF

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Aqua Security – Aqua Cloud Native Security Platform

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/aquasecurity/aquasecurity`

Aqua Cloud Native Security Platform (CSP) bietet Sicherheit über den gesamten Lebenszyklus von containerbasierten und serverlosen Anwendungen, von Ihrer CI/CD Pipeline bis hin zu Runtime-Produktionsumgebungen.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Aqua Security – Kube-bench

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/aqua-security/kube-bench`

Kube-bench ist ein Open-Source-Tool, das den Kubernetes-Benchmark des Center for Internet Security (CIS) in Ihrer Umgebung ausführt.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Armor – Armor Anywhere

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:679703615338:product/armordefense/armoranywhere`

Armor Anywhere bietet verwaltete Sicherheit und Compliance für AWS.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

AttackIQ – AttackIQ

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/attackiq/attackiq-platform`

AttackIQ Plattform emuliert echtes gegnerisches Verhalten im Einklang mit dem MITRE ATT&CK Framework, um Ihre allgemeine Sicherheitslage zu validieren und zu verbessern.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Barracuda Networks – Cloud Security Guardian

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:151784055945:product/barracuda/cloudsecurityguardian`

Barracuda Cloud Security Sentry hilft Unternehmen dabei, beim Erstellen von Anwendungen in der Public Cloud und beim Verschieben von Workloads in die Public Cloud sicher zu bleiben.

[AWS Link zum Marketplace](#)

[Link zum Produkt](#)

BigID – BigID Enterprise

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/bigid/bigid-enterprise`

Das BigID Enterprise Privacy Management Platform hilft Unternehmen dabei, sensible Daten (PII) in all ihren Systemen zu verwalten und zu schützen.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Blue Hexagon— Blue Hexagon für AWS

Art der Integration: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/blue-hexagon/blue-hexagon-for-aws`

Blue Hexagon ist eine Plattform zur Erkennung von Bedrohungen in Echtzeit. Sie verwendet Deep-Learning-Prinzipien, um bekannte und unbekannte Bedrohungen, einschließlich Malware und Netzwerkanomalien, zu erkennen.

[AWS Link zum Marketplace](#)

[Dokumentation für Partner](#)

Check Point – CloudGuard IaaS

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:758245563457:product/checkpoint/cloudguard-iaas`

Check Point CloudGuard erweitert auf einfache Weise die umfassende Sicherheit zur Bedrohungsabwehr AWS und schützt gleichzeitig Ressourcen in der Cloud.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Check Point – CloudGuard Posture Management

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:634729597623:product/checkpoint/dome9-arc`

Eine SaaS-Plattform, die überprüfbare Cloud-Netzwerksicherheit, fortschrittlichen IAM-Schutz sowie umfassende Compliance und Governance bietet.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Claroty – xDome

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/claroty/xdome`

Claroty xDome hilft Unternehmen, ihre cyberphysischen Systeme im erweiterten Internet der Dinge (XIoT) in industriellen (OT), Gesundheits- (IoMT) und Unternehmensumgebungen (IoT) zu schützen.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Cloud Storage Security— Antivirus for Amazon S3

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/cloud-storage-security/antivirus-for-amazon-s3`

Cloud Storage Security bietet Cloud-native Anti-Malware- und Antivirenschans für Amazon S3 S3-Objekte.

Antivirus for Amazon S3 bietet Echtzeit- und geplante Scans von Objekten und Dateien in Amazon S3 auf Malware und Bedrohungen. Es bietet Transparenz und Problembehebung bei problematischen und infizierten Dateien.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Contrast Security – Contrast Assess

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/contrast-security/security-assess`

Contrast Security Contrast Assess ist ein IAST-Tool, das die Erkennung von Sicherheitslücken in Web-Apps und Microservices APIs in Echtzeit ermöglicht. Contrast Assess lässt sich in Security Hub CSPM integrieren, um zentrale Transparenz und Reaktionsfähigkeit für all Ihre Workloads zu gewährleisten.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

CrowdStrike – CrowdStrike Falcon

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:517716713836:product/crowdstrike/crowdstrike-falcon`

Der CrowdStrike Falcon einzelne, leichte Sensor vereint Virenschutz der nächsten Generation, Endpunkterkennung und -abwehr sowie eine rund um die Uhr verwaltete Suche in der Cloud.

[AWS Link zum Marketplace](#)

[Dokumentation für Partner](#)

CyberArk – Privileged Threat Analytics

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:749430749651:product/cyberark/cyberark-pta`

Privileged Threat Analytics Erfassung, Erkennung und Reaktion auf risikoreiche Aktivitäten und Verhaltensweisen privilegierter Konten, um laufende Angriffe einzudämmen.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Data Theorem – Data Theorem

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/data-theorem/api-cloud-web-secure`

Data Theorem scannt kontinuierlich Webanwendungen und Cloud-Ressourcen auf der Suche nach Sicherheitslücken und Datenschutzlücken, um AppSec Datenschutzverletzungen zu verhindern. APIs

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Drata

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/drata/drata-integration`

Drata ist eine Plattform zur Compliance-Automatisierung, mit der Sie die Einhaltung verschiedener Frameworks wie SOC2 ISO und GDPR erreichen und aufrechterhalten können. Die Integration zwischen Drata und Security Hub CSPM hilft Ihnen, Ihre Sicherheitserkenntnisse an einem Ort zu zentralisieren.

[AWS Link zum Marketplace](#)

[Dokumentation für Partner](#)

Forcepoint – Forcepoint CASB

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-casb`

Forcepoint CASB ermöglicht es Ihnen, die Nutzung von Cloud-Anwendungen zu ermitteln, Risiken zu analysieren und angemessene Kontrollen für SaaS- und benutzerdefinierte Anwendungen durchzusetzen.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Forcepoint – Forcepoint Cloud Security Gateway

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/forcepoint/forcepoint-cloud-security-gateway`

Forcepoint Cloud Security Gateway ist ein konvergenter Cloud-Sicherheitsdienst, der Transparenz, Kontrolle und Bedrohungsschutz für Benutzer und Daten bietet, egal wo sie sich befinden.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Forcepoint – Forcepoint DLP

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-dlp`

Forcepoint DLP begegnet Risiken, bei denen der Mensch im Mittelpunkt steht, und bietet Transparenz und Kontrolle überall dort, wo Ihre Mitarbeiter arbeiten und wo sich Ihre Daten befinden.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Forcepoint – Forcepoint NGFW

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-ngfw`

Forcepoint NGFW ermöglicht es Ihnen, Ihre AWS Umgebung mit Ihrem Unternehmensnetzwerk zu verbinden und bietet die Skalierbarkeit, den Schutz und die Einblicke, die Sie benötigen, um Ihr Netzwerk zu verwalten und auf Bedrohungen zu reagieren.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Fugue – Fugue

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/fugue/fugue`

Fugue ist eine skalierbare Cloud-native Plattform ohne Agenten, die die kontinuierliche Validierung von Cloud-Laufzeitumgebungen automatisiert infrastructure-as-code und dabei dieselben Richtlinien verwendet.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Guardicore – Centra 4.0

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/guardicore/guardicore`

Guardicore Centra bietet Flussvisualisierung, Mikrosegmentierung und Erkennung von Sicherheitslücken für Workloads in modernen Rechenzentren und Clouds.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

HackerOne – Vulnerability Intelligence

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/hackerone/vulnerability-intelligence`

Die HackerOne Plattform arbeitet mit der weltweiten Hacker-Community zusammen, um die wichtigsten Sicherheitsprobleme aufzudecken. Vulnerability Intelligence ermöglicht es Ihrem Unternehmen, über automatisiertes Scannen hinauszugehen. Es enthält Sicherheitslücken, die von HackerOne ethischen Hackern validiert und Schritte zur Reproduktion bereitgestellt wurden.

[AWS Link zum Marktplatz](#)

[Dokumentation für Partner](#)

JFrog – Xray

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/jfrog/jfrog-xray`

JFrog Xray ist ein universelles Tool zur Analyse der Anwendungssicherheit (Software Composition Analysis, SCA), das Binärdateien kontinuierlich auf Lizenzbestimmungen und Sicherheitslücken scannt, sodass Sie eine sichere Software-Lieferkette betreiben können.

[AWS Link zum Marketplace](#)

[Dokumentation für Partner](#)

Juniper Networks – vSRX Next Generation Firewall

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/juniper-networks/vsrx-next-generation-firewall`

Juniper Networks'vSRX Virtual Next Generation Firewall bietet eine vollständige cloudbasierte virtuelle Firewall mit erweiterter Sicherheit, sicherem SD-WAN, robustem Netzwerk und integrierter Automatisierung.

[AWS Link zum Marketplace](#)

[Dokumentation für Partner](#)

[Link zum Produkt](#)

k9 Security – Access Analyzer

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/k9-security/access-analyzer`

k9 Security benachrichtigt Sie, wenn wichtige Zugangsänderungen in Ihrem AWS Identity and Access Management Konto vorgenommen werden. Damit können Sie nachvollziehen, k9 Security, welchen Zugriff Benutzer und IAM-Rollen auf wichtige Daten AWS-Services und Ihre Daten haben.

k9 Security ist für Continuous Delivery konzipiert und ermöglicht Ihnen die Operationalisierung von IAM mit umsetzbaren Zugriffsprüfungen und einfacher Richtlinienautomatisierung für und Terraform. AWS CDK

[Link zum Produkt](#)[Dokumentation für Partner](#)

Lacework – Lacework

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/lacework/lacework`

Lacework ist die datengesteuerte Sicherheitsplattform für die Cloud. Die Lacework Cloud Security Platform automatisiert Cloud-Sicherheit in großem Maßstab, sodass Sie schnell und sicher innovieren können.

[Link zum Produkt](#)[Dokumentation für Partner](#)

McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws`

McAfee MVISION Cloud Native Application Protection Platform (CNAPP) bietet Cloud Security Posture Management (CSPM) und Cloud Workload Protection Platform (CWPP) für Ihre Umgebung. AWS

[Link zum Produkt](#)[Dokumentation für Partner](#)

NETSCOUT – NETSCOUT Cyber Investigator

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/netscout/netscout-cyber-investigator`

NETSCOUT Cyber Investigator ist eine unternehmensweite Plattform für Netzwerkbedrohungen, Risikountersuchungen und forensische Analysen, die dazu beiträgt, die Auswirkungen von Cyberbedrohungen auf Unternehmen zu verringern.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Palo Alto Networks – Prisma Cloud Compute

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:496947949261:product/twistlock/twistlock-enterprise`

Prisma Cloud Compute ist eine Cloud-native Cybersicherheitsplattform VMs, die Container und serverlose Plattformen schützt.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Palo Alto Networks – Prisma Cloud Enterprise

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:188619942792:product/paloaltonetworks/redlock`

Schützt Ihre AWS Bereitstellung mit Cloud-Sicherheitsanalysen, fortschrittlicher Bedrohungserkennung und Compliance-Überwachung.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Plerion – Cloud Security Platform

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/plerion/cloud-security-platform`

Plerion ist eine Cloud-Sicherheitsplattform mit einem einzigartigen, bedrohungsorientierten, risikoorientierten Ansatz, der präventive, detektive und korrektive Maßnahmen für Ihre Workloads

bietet. Die Integration zwischen Plerion und Security Hub CSPM ermöglicht es Kunden, ihre Sicherheitsergebnisse an einem Ort zu zentralisieren und entsprechend zu handeln.

[AWS Link zum Marketplace](#)

[Dokumentation für Partner](#)

Prowler – Prowler

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/prowler/prowler`

Prowler ist ein Open-Source-Sicherheitstool zur Durchführung von AWS Prüfungen in Bezug auf bewährte Sicherheitsverfahren, Schutzmaßnahmen und kontinuierliche Überwachung.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Qualys – Vulnerability Management

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:805950163170:product/qualys/qualys-vm`

Qualys Vulnerability Management (VM) scannt und identifiziert kontinuierlich Sicherheitslücken und schützt so Ihre Ressourcen.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Rapid7 – InsightVM

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:336818582268:product/rapid7/insightvm`

Rapid7 InsightVM bietet Schwachstellenmanagement für moderne Umgebungen, sodass Sie Sicherheitslücken effizient finden, priorisieren und beheben können.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

SecureCloudDB – SecureCloudDB

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/secureclouddb/secureclouddb`

SecureCloudDB ist ein Cloud-natives Datenbanksicherheitstool, das einen umfassenden Überblick über interne und externe Sicherheitslage und -aktivitäten bietet. Es weist auf Sicherheitsverletzungen hin und behebt ausnutzbare Datenbankschwachstellen.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

SentinelOne – SentinelOne

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/sentinelone/endpoint-protection`

SentinelOne ist eine autonome XDR-Plattform (Extended Detection and Response), die KI-gestützte Prävention, Erkennung, Reaktion und Suche über Endpunkte, Container, Cloud-Workloads und IoT-Geräte hinweg umfasst.

[AWS Link zum Marketplace](#)

[Link zum Produkt](#)

Snyk

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/snyk/snyk`

Snyk bietet eine Sicherheitsplattform, die App-Komponenten auf Sicherheitsrisiken in Workloads überprüft, auf AWS denen sie ausgeführt werden. Diese Risiken werden als Ergebnisse an Security

Hub CSPM gesendet, sodass Entwickler und Sicherheitsteams sie zusammen mit den übrigen Sicherheitsergebnissen visualisieren und priorisieren können AWS .

[AWS Link zum Marketplace](#)

[Dokumentation für Partner](#)

Sonrai Security – Sonrai Dig

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/sonrai-security/sonrai-dig`

Sonrai Digüberwacht und behebt Cloud-Fehlkonfigurationen und Richtlinienverstöße, sodass Sie Ihren Sicherheits- und Compliance-Status verbessern können.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Sophos – Server Protection

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:062897671886:product/sophos/sophos-server-protection`

Sophos Server Protection schützt die kritischen Anwendungen und Daten, die das Herzstück Ihres Unternehmens bilden, mithilfe umfassender defense-in-depth Techniken.

[Link zum Produkt](#)

StackRox – StackRox Kubernetes Security

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/stackrox/kubernetes-security`

StackRox hilft Unternehmen dabei, ihre Container- und Kubernetes-Implementierungen in großem Umfang zu sichern, indem sie ihre Compliance- und Sicherheitsrichtlinien über den gesamten Container-Lebenszyklus hinweg durchsetzen — bei der Erstellung, Bereitstellung und Ausführung.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Sumo Logic – Machine Data Analytics

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:956882708938:product/sumologicinc/sumologic-mda`

Sumo Logic ist eine sichere Plattform zur Analyse von Maschinendaten, mit der Entwicklungs- und Sicherheitsteams ihre AWS Anwendungen erstellen, ausführen und sichern können.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Symantec – Cloud Workload Protection

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:754237914691:product/symantec-corp/symantec-cwp`

Cloud Workload Protection bietet umfassenden Schutz für Ihre EC2 Amazon-Instances mit Malware-Schutz, Intrusion Prevention und Überwachung der Dateiintegrität.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Tenable – Tenable.io

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:422820575223:product/tenable/tenable-io`

Präzises Identifizieren, Untersuchen und Priorisieren von Schwachstellen. In der Cloud verwaltet.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Trend Micro – Cloud One

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/trend-micro/cloud-one`

Trend Micro Cloud One stellt Teams zur richtigen Zeit und am richtigen Ort die richtigen Sicherheitsinformationen zur Verfügung. Diese Integration sendet Sicherheitsergebnisse in Echtzeit an Security Hub CSPM und verbessert so die Sichtbarkeit Ihrer AWS Ressourcen und Trend Micro Cloud One Ereignisdetails in Security Hub CSPM.

[AWS Link zum Marketplace](#)[Dokumentation für Partner](#)

Vectra – Cognito Detect

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:978576646331:product/vectra-ai/cognito-detect`

Vectra verändert die Cybersicherheit, indem es fortschrittliche KI einsetzt, um versteckte Cyberangreifer zu erkennen und darauf zu reagieren, bevor sie stehlen oder Schaden anrichten können.

[AWS Link zum Marketplace](#)[Dokumentation für Partner](#)

Wiz – Wiz Security

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/wiz-security/wiz-security`

Wiz analysiert kontinuierlich Konfigurationen, Sicherheitslücken, Netzwerke, IAM-Einstellungen, Geheimnisse und mehr für Sie AWS-Konten, Benutzer und Workloads, um kritische Probleme zu

entdecken, die ein echtes Risiko darstellen. Integrieren Sie Wiz in Security Hub CSPM, um Probleme zu visualisieren und darauf zu reagieren, die Wiz von der Security Hub CSPM-Konsole aus erkennt.

[AWS Link zum Marketplace](#)

[Dokumentation für Partner](#)

Integrationen von Drittanbietern, die Ergebnisse von Security Hub CSPM erhalten

Die folgenden Produktintegrationen von Drittanbietern können Ergebnisse von Security Hub CSPM erhalten. Sofern angegeben, aktualisiert das Produkt möglicherweise auch die Ergebnisse. In diesem Fall werden Aktualisierungen, die Sie an den Ergebnissen des Partnerprodukts vornehmen, auch in Security Hub CSPM widerspiegelt.

Atlassian - Jira Service Management

Integrationstyp: Empfangen und aktualisieren

Das AWS Service Management Connector for Jira sendet Ergebnisse von Security Hub CSPM an. Jira Probleme werden auf der Grundlage der Ergebnisse erstellt. Wenn die Jira Probleme aktualisiert werden, werden die entsprechenden Ergebnisse in Security Hub CSPM aktualisiert.

Die Integration unterstützt nur Jira Server und Jira Data Center.

Einen Überblick über die Integration und ihre Funktionsweise finden Sie im Video [AWS Security Hub Cloud Security Posture Management \(CSPM\) — Bidirektionale](#) Integration mit. Atlassian Jira Service Management

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Atlassian - Jira Service Management Cloud

Integrationstyp: Empfangen und aktualisieren

Jira Service Management Cloud ist die Cloud-Komponente von Jira Service Management.

Das AWS Service Management Connector for Jira sendet Ergebnisse von Security Hub CSPM an. Jira Die Ergebnisse lösen die Entstehung von Problemen in aus. Jira Service Management

Cloud Wenn Sie diese Probleme in aktualisierenJira Service Management Cloud, werden die entsprechenden Ergebnisse auch in Security Hub CSPM aktualisiert.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Atlassian – Opsgenie

Integrationstyp: Empfangen

Opsgenie ist eine moderne Incident-Management-Lösung für den Betrieb ständig verfügbarer Dienste, die es Entwicklungs- und Betriebsteams ermöglicht, Serviceunterbrechungen zu planen und bei Vorfällen die Kontrolle zu behalten.

Durch die Integration mit Security Hub CSPM wird sichergestellt, dass geschäftskritische sicherheitsrelevante Vorfälle zur sofortigen Lösung an die entsprechenden Teams weitergeleitet werden.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Dynatrace

Integrationstyp: Empfangen

Die Dynatrace Integration mit Security Hub CSPM hilft dabei, Sicherheitserkenntnisse in allen Tools und Umgebungen zu vereinheitlichen, zu visualisieren und zu automatisieren. Das Hinzufügen von Dynatrace Laufzeitkontexten zu den Sicherheitsergebnissen ermöglicht eine intelligentere Priorisierung, trägt dazu bei, die durch Warnmeldungen verursachten Störungen zu reduzieren und Ihre DevSecOps Teams darauf zu konzentrieren, die kritischen Probleme, die Ihre Produktionsumgebungen und Anwendungen betreffen, effizient zu beheben.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Fortinet – FortiCNP

Integrationstyp: Empfangen

FortiCNPist ein Cloud-Native-Protection-Produkt, das Sicherheitserkenntnisse zu umsetzbaren Erkenntnissen zusammenfasst und Sicherheitsinformationen auf der Grundlage der Risikobewertung priorisiert, um Alarmermüdung zu reduzieren und Problembehebungen zu beschleunigen.

[AWS Link zum Marketplace](#)

[Dokumentation für Partner](#)

IBM – QRadar

Integrationstyp: Empfangen

IBM QRadarSIEM bietet Sicherheitsteams die Möglichkeit, Bedrohungen schnell und präzise zu erkennen, zu priorisieren, zu untersuchen und darauf zu reagieren.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Logz.io Cloud SIEM

Integrationstyp: Empfangen

Logz.ioist ein AnbieterCloud SIEM, der eine erweiterte Korrelation von Protokoll- und Ereignisdaten bereitstellt, um Sicherheitsteams dabei zu unterstützen, Sicherheitsbedrohungen in Echtzeit zu erkennen, zu analysieren und darauf zu reagieren.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

MetricStream – CyberGRC

Integrationstyp: Empfangen

MetricStream CyberGRChilft Ihnen bei der Verwaltung, Messung und Minderung von Cybersicherheitsrisiken. Durch den Erhalt der CSPM-Ergebnisse von Security Hub erhalten Sie CyberGRC einen besseren Einblick in diese Risiken, sodass Sie Investitionen in Cybersicherheit priorisieren und IT-Richtlinien einhalten können.

[AWS Link zum Marketplace](#)

[Link zum Produkt](#)

MicroFocus – MicroFocus Arcsight

Integrationstyp: Empfangen

ArcSightbeschleunigt die effektive Erkennung und Reaktion auf Bedrohungen in Echtzeit und integriert dabei die Korrelation von Ereignissen sowie überwachte und unbeaufsichtigte Analysen mit der Automatisierung und Orchestrierung von Reaktionen.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

New Relic Vulnerability Management

Integrationstyp: Empfangen

New Relic Vulnerability Managementempfängt Sicherheitsergebnisse von Security Hub CSPM, sodass Sie einen zentralen Überblick über die Sicherheit und die Leistungstelemetrie im Kontext Ihres gesamten Stacks erhalten.

[AWS Link zum Marketplace](#)

[Dokumentation für Partner](#)

PagerDuty – PagerDuty

Integrationstyp: Empfangen

Die PagerDuty digitale Betriebsmanagement-Plattform ermöglicht es Teams, proaktiv Probleme zu lösen, die sich auf Kunden auswirken, indem jedes Signal automatisch in die richtigen Erkenntnisse und Maßnahmen umgewandelt wird.

AWS Benutzer können die PagerDuty Reihe von AWS Integrationen nutzen, um ihre AWS und hybride Umgebungen vertrauensvoll zu skalieren.

In Verbindung mit den aggregierten und organisierten Sicherheitswarnungen von Security Hub CSPM PagerDuty können Teams ihren Prozess zur Reaktion auf Bedrohungen automatisieren und schnell benutzerdefinierte Aktionen einrichten, um potenziellen Problemen vorzubeugen.

PagerDutyBenutzer, die ein Cloud-Migrationsprojekt durchführen, können schnell handeln und gleichzeitig die Auswirkungen von Problemen verringern, die während des Migrationszyklus auftreten.

[Link zum Produkt](#)[Dokumentation für Partner](#)

Palo Alto Networks – Cortex XSOAR

Integrationstyp: Empfangen

Cortex XSOAR ist eine SOAR-Plattform (Security Orchestration, Automation and Response), die sich in Ihr gesamtes Sicherheitsprodukteportfolio integrieren lässt, um die Reaktion auf Vorfälle und die Sicherheitsabläufe zu beschleunigen.

[Link zum Produkt](#)[Dokumentation für Partner](#)

Palo Alto Networks – VM-Series

Integrationstyp: Empfangen

Palo Alto VM-Series Die Integration mit Security Hub CSPM sammelt Bedrohungsinformationen und sendet sie als automatische Aktualisierung der Sicherheitsrichtlinien an die Firewall der VM-Series nächsten Generation, die böswillige IP-Adressaktivitäten blockiert.

[Link zum Produkt](#)[Dokumentation für Partner](#)

Rackspace Technology – Cloud Native Security

Integrationstyp: Empfangen

Rackspace Technology bietet zusätzlich zu systemeigenen Sicherheitsprodukten verwaltete AWS Sicherheitsdienste für die Überwachung rund um die Uhr durch Rackspace SOC, erweiterte Analysen und die Beseitigung von Bedrohungen.

[Link zum Produkt](#)

Rapid7 – InsightConnect

Integrationstyp: Empfangen

Rapid7 InsightConnect ist eine Lösung zur Sicherheitsorchestrierung und Automatisierung, mit der Ihr Team den SOC-Betrieb mit wenig bis gar keinem Code optimieren kann.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

RSA – RSA Archer

Integrationstyp: Empfangen

RSA Archer Mit IT- und Sicherheitsrisikomanagement können Sie ermitteln, welche Ressourcen für Ihr Unternehmen von entscheidender Bedeutung sind, Sicherheitsrichtlinien und -standards festlegen und kommunizieren, Angriffe erkennen und darauf reagieren, Sicherheitsmängel erkennen und beheben sowie klare Best Practices für das IT-Risikomanagement festlegen.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

ServiceNow – ITSM

Integrationstyp: Empfangen und aktualisieren

ServiceNow Durch die Integration mit Security Hub CSPM können die Sicherheitsergebnisse von Security Hub CSPM darin eingesehen werden. ServiceNow ITSM Sie können auch so konfigurieren ServiceNow, dass automatisch ein Vorfall oder ein Problem erstellt wird, wenn es einen Befund von Security Hub CSPM erhält.

Alle Aktualisierungen dieser Vorfälle und Probleme führen zu Aktualisierungen der Ergebnisse in Security Hub CSPM.

Einen Überblick über die Integration und ihre Funktionsweise finden Sie im Video [AWS Security Hub Cloud Security Posture Management \(CSPM\) — Bidirektionale](#) Integration mit ServiceNow ITSM

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Slack – Slack

Integrationstyp: Empfangen

Slack ist eine Ebene des Technologie-Stacks für Unternehmen, die Menschen, Daten und Anwendungen zusammenbringt. Es ist ein zentraler Ort, an dem Menschen effektiv zusammenarbeiten, wichtige Informationen finden und auf Hunderttausende kritischer Anwendungen und Services zugreifen können, um Spitzenleistungen zu erbringen.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Splunk – Splunk Enterprise

Integrationstyp: Empfangen

Splunk verwendet Amazon CloudWatch Events als Nutzer von Security Hub CSPM-Ergebnissen. Senden Sie Ihre Daten Splunk für erweiterte Sicherheitsanalysen und SIEM an.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Splunk – Splunk Phantom

Integrationstyp: Empfangen

Mit der Splunk Phantom Anwendung für AWS Security Hub Cloud Security Posture Management (CSPM) werden die Ergebnisse Phantom zur automatisierten Kontextanreicherung mit zusätzlichen Threat-Intelligence-Informationen oder zur Durchführung automatisierter Reaktionsmaßnahmen gesendet.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

ThreatModeler

Integrationstyp: Empfangen

ThreatModeler ist eine automatisierte Lösung zur Bedrohungsmodellierung, die den Lebenszyklus von Unternehmenssoftware und Cloud-Entwicklung schützt und skaliert.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Trellix – Trellix Helix

Integrationstyp: Empfangen

Trellix Helix ist eine in der Cloud gehostete Plattform für Sicherheitsoperationen, die es Unternehmen ermöglicht, die Kontrolle über jeden Vorfall von der Warnung bis zur Behebung zu übernehmen.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Integrationen von Drittanbietern, die Ergebnisse an Security Hub CSPM senden und Ergebnisse von Security Hub empfangen

Die folgenden Produktintegrationen von Drittanbietern können Ergebnisse an Security Hub CSPM senden und Ergebnisse von Security Hub CSPM empfangen.

Caveonix – Caveonix Cloud

Integrationstyp: Senden und Empfangen

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/caveonix/caveonix-cloud`

Die Caveonix KI-gestützte Plattform automatisiert Transparenz, Bewertung und Risikominderung in Hybrid-Clouds und deckt Cloud-native Dienste und Container ab. VMs integriert in AWS Security Hub Cloud Security Posture Management (CSPM), Caveonix führt es AWS Daten und erweiterte Analysen zusammen, um Einblicke in Sicherheitswarnungen und Compliance zu erhalten.

[AWS Link zum Marketplace](#)

[Dokumentation für Partner](#)

Cloud Custodian – Cloud Custodian

Integrationstyp: Senden und Empfangen

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/cloud-custodian/cloud-custodian`

Cloud Custodian ermöglicht es Benutzern, in der Cloud gut verwaltet zu werden. Das einfache YAML-DSL ermöglicht einfach zu definierende Regeln, um eine gut verwaltete Cloud-Infrastruktur zu ermöglichen, die sowohl sicher als auch kostenoptimiert ist.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

DisruptOps, Inc. – DisruptOPS

Integrationstyp: Senden und Empfangen

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/disruptops-inc/disruptops`

Die DisruptOps Security Operations Platform unterstützt Unternehmen dabei, mithilfe automatisierter Leitplanken die besten Sicherheitspraktiken in Ihrer Cloud aufrechtzuerhalten.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Kion

Integrationstyp: Senden und Empfangen

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/cloudtamerio/cloudtamerio`

Kion(ehmals cloudtamer.io) ist eine komplette Cloud-Governance-Lösung für. AWSKionbietet Stakeholdern Einblick in den Cloud-Betrieb und hilft Cloud-Nutzern dabei, Konten zu verwalten, Budget und Kosten zu kontrollieren und die kontinuierliche Einhaltung von Vorschriften sicherzustellen.

[Link zum Produkt](#)

[Dokumentation für Partner](#)

Turbot – Turbo

Integrationstyp: Senden und Empfangen

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/turbot/turbot`

Turbotstellt sicher, dass Ihre Cloud-Infrastruktur sicher, konform, skalierbar und kostenoptimiert ist.

[Link zum Produkt](#)[Dokumentation für Partner](#)

Integration von Security Hub CSPM mit kundenspezifischen Produkten

Zusätzlich zu den Ergebnissen, die durch integrierte AWS Dienste und Produkte von Drittanbietern generiert wurden, kann AWS Security Hub Cloud Security Posture Management (CSPM) auch Erkenntnisse nutzen, die von anderen kundenspezifischen Sicherheitsprodukten generiert wurden.

Sie können diese Ergebnisse mithilfe der Security Hub CSPM-API an [BatchImportFindings](#) Security Hub CSPM senden. Sie können denselben Vorgang verwenden, um Ergebnisse von benutzerdefinierten Produkten zu aktualisieren, die Sie bereits an Security Hub CSPM gesendet haben.

Verwenden Sie bei der Einrichtung der benutzerdefinierten Integration die [Richtlinien und Checklisten](#) im Security Hub CSPM Partner Integration Guide.

Anforderungen und Empfehlungen für kundenspezifische Produktintegrationen

Bevor Sie den [BatchImportFindings](#) API-Vorgang erfolgreich aufrufen können, müssen Sie Security Hub CSPM aktivieren.

Sie müssen außerdem mithilfe von Suchdetails für das benutzerdefinierte Produkt angeben. [the section called "Suchformat: ASFF"](#) Lesen Sie die folgenden Anforderungen und Empfehlungen für kundenspezifische Produktintegrationen:

Einstellen des Produkt-ARNs

Wenn Sie Security Hub CSPM aktivieren, wird ein Standardprodukt Amazon Resource Name (ARN) für Security Hub CSPM in Ihrem aktuellen Konto generiert.

Dieser Produkt-ARN weist das folgende Format auf:

`arn:aws:securityhub:<region>:<account-id>:product/<account-id>/default.`
Beispiel, `arn:aws:securityhub:us-west-2:123456789012:product/123456789012/default.`

Verwenden Sie diesen Produkt-ARN als Wert für das [ProductArn](#)-Attribut, wenn Sie die `BatchImportFindings`-API-Operation aufrufen.

Festlegung der Firmen- und Produktnamen

Sie können `BatchImportFindings` damit einen bevorzugten Firmen- und Produktnamen für die benutzerdefinierte Integration festlegen, die Ergebnisse an Security Hub CSPM sendet.

Ihre angegebenen Namen ersetzen den vorkonfigurierten Firmennamen und den Produktnamen, genannt persönlicher Name bzw. Standardname, und werden in der Security Hub CSPM-Konsole und in der JSON jedes Ergebnisses angezeigt. Siehe [BatchImportFindings um Anbieter zu finden](#).

Festlegung des Ergebnisses IDs

Sie müssen Ihr eigenes Ergebnis mithilfe des [Id](#)-Attributs angeben IDs, verwalten und erhöhen.

Jeder neue Befund sollte eine eindeutige Ergebnis-ID haben. Wenn das benutzerdefinierte Produkt mehrere Ergebnisse mit derselben Befund-ID sendet, verarbeitet Security Hub CSPM nur den ersten Befund.

Einstellen der Konto-ID

Sie müssen mit dem [AwsAccountId](#)-Attribut Ihre eigene Konto-ID angeben.

Einstellen Erstellungs- und Aktualisierungsdatums

Sie müssen eigene Zeitstempel für die Attribute [CreatedAt](#) und [UpdatedAt](#) angeben.

Importieren von Ergebnissen aus benutzerdefinierten Produkten

Zusätzlich zum Senden neuer Ergebnisse aus benutzerdefinierten Produkten können Sie auch die [BatchImportFindings](#)-API-Operation verwenden, um vorhandene Ergebnisse aus benutzerdefinierten Produkten zu aktualisieren.

Um vorhandene Ergebnisse zu aktualisieren, verwenden Sie die vorhandene Ergebnis-ID (über das [Id](#)-Attribut). Senden Sie das vollständige Ergebnis erneut mit den entsprechenden Informationen, die in der Anforderung aktualisiert wurden, einschließlich eines geänderten [UpdatedAt](#)-Zeitstempels.

Beispiel für benutzerdefinierte Integrationen

Sie können das folgende Beispiel für benutzerdefinierte Produktintegrationen als Leitfaden verwenden, um Ihre eigenen maßgeschneiderten Lösungen zu erstellen:

Ergebnisse von Chef InSpec Scans an Security Hub CSPM senden

Sie können eine AWS CloudFormation Vorlage erstellen, die einen [Chef InSpec](#) Konformitätsscan durchführt und die Ergebnisse dann an Security Hub CSPM sendet.

Weitere Informationen finden Sie unter [Kontinuierliche Compliance-Überwachung mit Chef InSpec und AWS Security Hub Cloud Security Posture Management \(CSPM\)](#).

Von entdeckte Container-Schwachstellen Trivy an Security Hub CSPM senden

Sie können eine AWS CloudFormation Vorlage erstellen, mit der Container [AquaSecurity Trivy](#) nach Sicherheitslücken gescannt werden, und die gefundenen Sicherheitslücken dann an Security Hub CSPM gesendet werden.

Weitere Informationen finden Sie unter [Aufbau einer CI/CD Pipeline für Container-Schwachstellenscans mit Trivy und AWS Security Hub Cloud Security Posture Management \(CSPM\)](#).

Ergebnisse in Security Hub CSPM erstellen und aktualisieren

In AWS Security Hub Cloud Security Posture Management (CSPM) ist ein Ergebnis eine beobachtbare Aufzeichnung einer Sicherheitsüberprüfung oder sicherheitsrelevanter Erkennung. Ein Befund kann aus einer der folgenden Quellen stammen:

- Eine Sicherheitsüberprüfung für ein Steuerelement in Security Hub CSPM.
- Eine Integration mit einem anderen AWS-Service
- Eine Integration mit einem Drittanbieterprodukt.
- Eine benutzerdefinierte Integration.

Security Hub CSPM normalisiert Ergebnisse aus allen Quellen in eine Standardsyntax und ein Standardformat, das als AWS Security Finding Format (ASFF) bezeichnet wird. Ausführliche Informationen zu diesem Format, einschließlich Beschreibungen der einzelnen ASFF-Felder, finden Sie unter [AWS Format für Sicherheitssuche \(ASFF\)](#). Wenn Sie die regionsübergreifende Aggregation aktivieren, aggregiert Security Hub CSPM auch automatisch neue und aktualisierte Ergebnisse aus allen verknüpften Regionen in eine von Ihnen angegebene Aggregationsregion. Weitere Informationen finden Sie unter [Grundlegendes zur regionsübergreifenden Aggregation in Security Hub CSPM](#).

Nachdem ein Ergebnis erstellt wurde, kann es wie folgt aktualisiert werden:

- Ein Findungsanbieter kann den [BatchImportFindings](#) Betrieb der Security Hub CSPM-API verwenden, um allgemeine Informationen über das Ergebnis zu aktualisieren. Ergebnisanbieter können nur Ergebnisse aktualisieren, die sie erstellt haben.
- Ein Kunde kann die Security Hub CSPM-Konsole oder den [BatchUpdateFindings](#) Betrieb der Security Hub CSPM-API verwenden, um den Status der Untersuchung des Ergebnisses zu aktualisieren. Der BatchUpdateFindings Vorgang kann auch von einem SIEM-, Ticketing-, Incident Management-, SOAR- oder anderen Tools im Namen eines Kunden genutzt werden.

Security Hub CSPM löscht automatisch Ergebnisse, die in letzter Zeit nicht aktualisiert wurden, um das Auffinden zu reduzieren und die Nachverfolgung und Analyse einzelner Ergebnisse zu optimieren. Der Zeitpunkt, zu dem Security Hub CSPM dies tut, hängt davon ab, ob ein Ergebnis aktiv oder archiviert ist:

- Ein aktives Ergebnis ist ein Befund, dessen Datensatzstatus (RecordState) ist. ACTIVE Security Hub CSPM speichert aktive Ergebnisse 90 Tage lang. Wenn ein aktives Ergebnis 90 Tage lang nicht aktualisiert wurde, läuft es ab und Security Hub CSPM löscht es dauerhaft.
- Ein archiviertes Ergebnis ist ein Befund mit dem Datensatzstatus (RecordState) ARCHIVED Security Hub CSPM speichert archivierte Ergebnisse 30 Tage lang. Wenn ein archiviertes Ergebnis 30 Tage lang nicht aktualisiert wurde, läuft es ab und Security Hub CSPM löscht es dauerhaft.

Bei Kontrollergebnissen, d. h. Ergebnissen, die Security Hub CSPM aus Sicherheitsprüfungen für Kontrollen generiert, bestimmt Security Hub CSPM anhand des Werts für das UpdatedAt Feld des Ergebnisses, ob ein Ergebnis abgelaufen ist. Wenn dieser Wert für einen aktiven Befund mehr als 90 Tage zurückliegt, löscht Security Hub CSPM den Befund dauerhaft. Wenn dieser Wert für einen archivierten Befund vor mehr als 30 Tagen lag, löscht Security Hub CSPM den Befund dauerhaft.

Für alle anderen Arten von Ergebnissen bestimmt Security Hub CSPM anhand der Werte für die UpdatedAt Felder ProcessedAt und des Ergebnisses, ob ein Ergebnis abgelaufen ist. Security Hub CSPM vergleicht die Werte für diese Felder und ermittelt, welcher aktueller ist. Wenn der neuere Wert für einen aktiven Befund vor mehr als 90 Tagen liegt, löscht Security Hub CSPM den Befund dauerhaft. Wenn der neuere Wert für ein archiviertes Ergebnis mehr als 30 Tage zurückliegt, löscht Security Hub CSPM das Ergebnis dauerhaft. Die Suche nach Anbietern kann den Wert für das UpdatedAt Feld eines oder mehrerer Ergebnisse mithilfe der [BatchImportFindings](#) Security Hub CSPM-API ändern.

Für eine längerfristige Aufbewahrung von Ergebnissen können Sie Ergebnisse in einen S3-Bucket exportieren. Sie können dies tun, indem Sie eine benutzerdefinierte Aktion mit einer EventBridge Amazon-Regel verwenden. Weitere Informationen finden Sie unter [Verwendung EventBridge für automatisierte Reaktionen und Problembehebungen](#).

Themen

- [BatchImportFindings um Anbieter zu finden](#)
- [BatchUpdateFindings für Kunden](#)
- [Überprüfung der Funddetails und des Verlaufs in Security Hub CSPM](#)
- [Ergebnisse im Security Hub CSPM filtern](#)
- [Gruppierung der Ergebnisse in Security Hub CSPM](#)
- [Den Workflow-Status von Ergebnissen in Security Hub CSPM festlegen](#)
- [Ergebnisse an eine benutzerdefinierte Security Hub CSPM-Aktion senden](#)
- [AWS Format für Sicherheitssuche \(ASFF\)](#)

BatchImportFindings um Anbieter zu finden

Die Suche nach Anbietern kann den [BatchImportFindings](#) Vorgang nutzen, um neue Erkenntnisse in AWS Security Hub Cloud Security Posture Management (CSPM) zu gewinnen. Sie können diesen Vorgang auch verwenden, um die von ihnen erstellten Ergebnisse zu aktualisieren. Die Suche nach Anbietern kann keine Ergebnisse aktualisieren, die sie nicht selbst erstellt haben.

Kunden SIEMs, Ticketverkauf, SOAR und andere Arten von Tools müssen den [BatchUpdateFindings](#) Vorgang verwenden, um Aktualisierungen im Zusammenhang mit ihrer Untersuchung der Ergebnisse aus der Suche nach Anbietern vorzunehmen. Weitere Informationen finden Sie unter [the section called "BatchUpdateFindings für Kunden"](#).

Wenn Security Hub CSPM eine BatchImportFindings Anfrage zur Erstellung oder Aktualisierung eines Ergebnisses erhält, generiert es automatisch ein Security Hub Findings - Imported Ereignis in Amazon. EventBridge Sie können bei diesem Ereignis automatisierte Maßnahmen ergreifen. Weitere Informationen finden Sie unter [the section called "Automatisierte Reaktion und Problembehebung"](#).

Voraussetzungen für die Verwendung von **BatchImportFindings**

BatchImportFindings muss von einer der folgenden Personen aufgerufen werden:

- Das Konto, das mit den Ergebnissen verknüpft ist. Die Kennung des verknüpften Kontos muss mit dem Wert des `AwsAccountId` Attributs für den Befund übereinstimmen.
- Ein Konto, das als offizielle Security Hub CSPM-Partnerintegration zugelassen ist.

Security Hub CSPM kann nur die Suche nach Updates für Konten akzeptieren, für die Security Hub CSPM aktiviert ist. Der Ergebnisanbieter muss ebenfalls aktiviert sein. Wenn Security Hub CSPM deaktiviert oder die Finding Provider-Integration nicht aktiviert ist, werden die Ergebnisse in der `FailedFindings` Liste mit einem `InvalidAccess` Fehler zurückgegeben.

Festlegen, ob ein Ergebnis erstellt oder aktualisiert werden soll

Um festzustellen, ob ein Ergebnis erstellt oder aktualisiert werden soll, überprüft Security Hub CSPM das `ID` Feld. Wenn der Wert von `ID` nicht mit einem vorhandenen Ergebnis übereinstimmt, erstellt Security Hub CSPM ein neues Ergebnis.

Wenn es `ID` mit einem vorhandenen Ergebnis übereinstimmt, überprüft Security Hub CSPM das `UpdatedAt` Feld auf das Update und geht wie folgt vor:

- Wenn das Update mit UpdatedAt dem vorhandenen Ergebnis übereinstimmt oder davor UpdatedAt auftritt, ignoriert Security Hub CSPM die Aktualisierungsanfrage.
- Wenn UpdatedAt das Update nach UpdatedAt dem vorhandenen Befund erfolgt, aktualisiert Security Hub CSPM den vorhandenen Befund.

Einschränkungen beim Auffinden von Updates mit **BatchImportFindings**

Die Suche nach Anbietern kann nicht verwendet BatchImportFindings werden, um die folgenden Attribute eines vorhandenen Ergebnisses zu aktualisieren:

- Note
- UserDefinedFields
- VerificationState
- Workflow

Security Hub CSPM ignoriert alle Inhalte, die in einer BatchImportFindings Anfrage für diese Attribute bereitgestellt werden. Kunden oder Organisationen, die in ihrem Namen handeln (z. B. Ticketing-Tools), können diese Attribute verwenden, BatchUpdateFindings um sie zu aktualisieren.

Aktualisierung der Ergebnisse mit FindingProviderFields

Finding Providers sollte außerdem nicht verwendet werden BatchImportFindings, um die folgenden Top-Level-Attribute im AWS Security Finding Format (ASFF) zu aktualisieren:

- Confidence
- Criticality
- RelatedFindings
- Severity
- Types

Stattdessen sollte die Suche nach Anbietern das [FindingProviderFields](#) Objekt verwenden, um Werte für diese Attribute bereitzustellen.

Beispiel

```
"FindingProviderFields": {
  "Confidence": 42,
  "Criticality": 99,
  "RelatedFindings": [
    {
      "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "123e4567-e89b-12d3-a456-426655440000"
    }
  ],
  "Severity": {
    "Label": "MEDIUM",
    "Original": "MEDIUM"
  },
  "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

Bei `BatchImportFindings` Anfragen verarbeitet Security Hub CSPM Werte in den Attributen der obersten Ebene und wie folgt. [FindingProviderFields](#)

(Preferred) **BatchImportFindings** liefert einen Wert für ein Attribut in [FindingProviderFields](#), aber keinen Wert für das entsprechende Attribut der obersten Ebene.

Zum Beispiel `BatchImportFindings` liefert `FindingProviderFields.Confidence`, aber nicht. `Confidence` Dies ist die bevorzugte Option für `BatchImportFindings` Anfragen.

Security Hub CSPM aktualisiert den Wert des Attributs in. `FindingProviderFields`

Es repliziert den Wert nur dann in das Attribut der obersten Ebene, wenn das Attribut nicht bereits von aktualisiert wurde. `BatchUpdateFindings`

BatchImportFindings liefert einen Wert für ein Attribut der obersten Ebene, aber keinen Wert für das entsprechende Attribut in. **FindingProviderFields**

Stellt beispielsweise `BatchImportFindings` bereit `Confidence`, liefert aber nicht. `FindingProviderFields.Confidence`

Security Hub CSPM verwendet den Wert, um das Attribut in zu aktualisieren. `FindingProviderFields` Es überschreibt jeden vorhandenen Wert.

Security Hub CSPM aktualisiert das Attribut der obersten Ebene nur, wenn das Attribut nicht bereits von aktualisiert wurde. `BatchUpdateFindings`

BatchImportFindings stellt einen Wert sowohl für ein Attribut der obersten Ebene als auch für das entsprechende Attribut in bereit. **FindingProviderFields**

BatchImportFindingsStellt beispielsweise sowohl als auch Confidence bereit.
FindingProviderFields.Confidence

Für ein neues Ergebnis verwendet Security Hub CSPM den Wert in, FindingProviderFields um sowohl das oberste Ebenenattribut als auch das entsprechende Attribut in aufzufüllen. FindingProviderFields Der angegebene Attributwert der obersten Ebene wird nicht verwendet.

Für ein vorhandenes Ergebnis verwendet Security Hub CSPM beide Werte. Der Attributwert der obersten Ebene wird jedoch nur aktualisiert, wenn das Attribut nicht bereits von aktualisiert wurde. BatchUpdateFindings

BatchUpdateFindings für Kunden

AWS Kunden von Security Hub Cloud Security Posture Management (CSPM) und Unternehmen, die in ihrem Namen handeln, können den [BatchUpdateFindings](#) Vorgang nutzen, um Informationen im Zusammenhang mit der Verarbeitung von Security Hub CSPM-Ergebnissen von suchenden Anbietern zu aktualisieren. Als Kunde können Sie diesen Vorgang direkt verwenden. SIEM-, Ticketing-, Incident Management- und SOAR-Tools können diesen Vorgang auch im Auftrag eines Kunden nutzen.

Sie können den BatchUpdateFindings Vorgang nicht verwenden, um neue Erkenntnisse zu gewinnen. Sie können ihn jedoch verwenden, um bis zu 100 vorhandene Ergebnisse gleichzeitig zu aktualisieren. In einer BatchUpdateFindings Anfrage geben Sie an, welche Ergebnisse aktualisiert werden sollen, welche ASFF-Felder (AWS Security Finding Format) für die Ergebnisse aktualisiert werden sollen, und die neuen Werte für die Felder. Security Hub CSPM aktualisiert dann die Ergebnisse wie in Ihrer Anfrage angegeben. Dieser Vorgang kann einige Minuten dauern. Wenn Sie die Ergebnisse mithilfe des BatchUpdateFindings Vorgangs aktualisieren, wirken sich Ihre Aktualisierungen nicht auf die vorhandenen Werte für das UpdatedAt Ergebnisfeld aus.

Wenn Security Hub CSPM eine BatchUpdateFindings Anfrage zur Aktualisierung eines Ergebnisses erhält, generiert es automatisch ein Security Hub Findings – Imported Ereignis in Amazon. EventBridge Sie können dieses Ereignis optional verwenden, um automatisierte Maßnahmen in Bezug auf das angegebene Ergebnis zu ergreifen. Weitere Informationen finden Sie unter [the section called “Automatisierte Reaktion und Problembehebung”](#).

Verfügbare Felder für BatchUpdateFindings

Wenn Sie mit einem Security Hub CSPM-Administratorkonto angemeldet sind, können Sie BatchUpdateFindings damit Ergebnisse aktualisieren, die vom Administratorkonto oder den Mitgliedskonten generiert wurden. Mitgliedskonten können nur BatchUpdateFindings zur Aktualisierung der Ergebnisse für ihr Konto verwendet werden.

Kunden können BatchUpdateFindings damit die folgenden Felder und Objekte aktualisieren:

- Confidence
- Criticality
- Note
- RelatedFindings
- Severity
- Types
- UserDefinedFields
- VerificationState
- Workflow

Konfiguration des Zugriffs auf BatchUpdateFindings

Sie können AWS Identity and Access Management (IAM-) Richtlinien konfigurieren, um den Zugriff auf die Verwendung BatchUpdateFindings zur Aktualisierung von Suchfeldern und Feldwerten einzuschränken.

Verwenden Sie in einer Anweisung, auf die der Zugriff beschränkt werden soll BatchUpdateFindings, die folgenden Werte:

- Action ist securityhub:BatchUpdateFindings
- Effect ist Deny
- Denn Condition Sie können eine BatchUpdateFindings Anfrage auf folgender Grundlage ablehnen:
 - Das Ergebnis umfasst ein bestimmtes Feld.
 - Das Ergebnis beinhaltet einen bestimmten Feldwert.

Bedingungsschlüssel

Dies sind die Bedingungsschlüssel für die Einschränkung des Zugriffs auf `BatchUpdateFindings`.

ASFF-Feld

Der Bedingungsschlüssel für ein ASFF-Feld lautet wie folgt:

```
securityhub:ASFFSyntaxPath/<fieldName>
```

Ersetzen Sie es `<fieldName>` durch das ASFF-Feld. Fügen Sie bei der Konfiguration des Zugriffs auf `BatchUpdateFindings` ein oder mehrere spezifische ASFF-Felder in Ihre IAM-Richtlinie ein und nicht ein Feld auf übergeordneter Ebene. Um beispielsweise den Zugriff auf das `Workflow.Status` Feld einzuschränken, müssen Sie es `securityhub:ASFFSyntaxPath/Workflow.Status` in Ihre Richtlinie aufnehmen und nicht das Feld auf übergeordneter Ebene.

Alle Aktualisierungen eines Felds verbieten

Um zu verhindern, dass ein Benutzer ein bestimmtes Feld aktualisiert, verwenden Sie eine Bedingung wie die folgende:

```
"Condition": {
    "Null": {
        "securityhub:ASFFSyntaxPath/<fieldName>": "false"
    }
}
```

Die folgende Aussage weist beispielsweise darauf hin, dass das `Workflow.Status` Ergebnisfeld nicht aktualisiert werden kann.

```
{
  "Sid": "VisualEditor0",
  "Effect": "Deny",
  "Action": "securityhub:BatchUpdateFindings",
  "Resource": "*",
  "Condition": {
    "Null": {
      "securityhub:ASFFSyntaxPath/Workflow.Status": "false"
    }
  }
}
```

```
}
}
```

Bestimmte Feldwerte nicht zulassen

Um zu verhindern, dass ein Benutzer ein Feld auf einen bestimmten Wert festlegt, verwenden Sie eine Bedingung wie die folgende:

```
"Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/<fieldName>": "<fieldValue>"
    }
}
```

Die folgende Anweisung weist beispielsweise darauf hin, dass diese Einstellung nicht verwendet werden BatchUpdateFindings kann, um auf Workflow.Status zu setzen SUPPRESSED.

```
{
  "Sid": "VisualEditor0",
  "Effect": "Deny",
  "Action": "securityhub:BatchUpdateFindings",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "securityhub:ASFFSyntaxPath/Workflow.Status": "SUPPRESSED"
    }
  }
}
```

Sie können auch eine Liste mit Werten angeben, die nicht zulässig sind.

```
"Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/<fieldName>": [ "<fieldValue1>",
        "<fieldValue2>", "<fieldValue3>" ]
    }
}
```

Die folgende Anweisung weist beispielsweise darauf hin, dass dieser Wert nicht verwendet werden BatchUpdateFindings kann, um entweder Workflow.Status auf RESOLVED oder zu setzen SUPPRESSED.

```
{
  "Sid": "VisualEditor0",
  "Effect": "Deny",
  "Action": "securityhub:BatchUpdateFindings",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "securityhub:ASFFSyntaxPath/Workflow.Status": [
        "RESOLVED",
        "NOTIFIED"
      ]
    }
  }
}
```

Überprüfung der Funddetails und des Verlaufs in Security Hub CSPM

In AWS Security Hub Cloud Security Posture Management (CSPM) ist ein Ergebnis eine beobachtbare Aufzeichnung einer Sicherheitsüberprüfung oder sicherheitsrelevanter Erkennung. Security Hub CSPM generiert ein Ergebnis, wenn es eine Sicherheitsüberprüfung einer Kontrolle abschließt und wenn es ein Ergebnis aus einem integrierten Produkt AWS-Service oder einem Drittanbieterprodukt aufnimmt. Jedes Ergebnis enthält eine Historie der Änderungen und weitere Details, wie z. B. eine Bewertung des Schweregrads und Informationen zu den betroffenen Ressourcen.

Sie können den Verlauf und andere Details einzelner Ergebnisse auf der Security Hub CSPM-Konsole oder programmgesteuert mit der Security Hub CSPM-API oder dem überprüfen. AWS CLI

Um Ihnen bei der Optimierung Ihrer Analyse zu helfen, zeigt die Security Hub CSPM-Konsole ein Ergebnisfenster an, wenn Sie ein bestimmtes Ergebnis auswählen. Das Fenster umfasst verschiedene Menüs und Registerkarten zur Überprüfung bestimmter Details eines Ergebnisses.

Menü „Aktionen“

In diesem Menü können Sie die vollständige JSON-Datei eines Befundes überprüfen oder Notizen hinzufügen. Einem Befund kann jeweils nur eine Notiz angehängt werden. Dieses Menü bietet auch Optionen, um [den Workflow-Status eines Ergebnisses festzulegen](#) oder [ein Ergebnis an eine benutzerdefinierte Aktion in Amazon zu senden](#) EventBridge.

Menü „Untersuchen“

In diesem Menü können Sie einen Befund in Amazon Detective untersuchen. Detective extrahiert Entitäten wie IP-Adressen und AWS Benutzer aus einem Befund und visualisiert deren Aktivitäten. Sie können die Entitätsaktivität als Ausgangspunkt verwenden, um die Ursache und die Auswirkung eines Ergebnisses zu untersuchen.

Registerkarte Overview (Übersicht)

Diese Registerkarte enthält eine Zusammenfassung eines Ergebnisses. Sie können beispielsweise ermitteln, wann ein Ergebnis erstellt und zuletzt aktualisiert wurde, in welchem Konto es vorhanden ist und aus welcher Quelle das Ergebnis stammt. Bei Kontrollergebnissen werden auf dieser Registerkarte auch der Name der zugehörigen AWS Config Regel und ein Link zu Anleitungen zur Problembehebung in der Security Hub CSPM-Dokumentation angezeigt.

Im Ressourcen-Snapshot auf der Registerkarte Übersicht können Sie sich einen kurzen Überblick über die Ressourcen verschaffen, die an einem Befund beteiligt waren. Bei einigen Ressourcen umfasst dies die Option „Ressource öffnen“, die direkt zu einer betroffenen Ressource auf der entsprechenden AWS-Service Konsole führt. Die Momentaufnahme des Verlaufs zeigt bis zu zwei Änderungen, die an dem Datum vorgenommen wurden, an dem der Verlauf zuletzt erfasst wurde. Wenn Sie beispielsweise gestern eine Änderung und heute eine weitere vorgenommen haben, zeigt der Snapshot die Änderung von heute. Um frühere Einträge zu überprüfen, wechseln Sie zur Registerkarte Verlauf.

Die Zeile Konformität wird erweitert, um weitere Details anzuzeigen. Wenn ein Steuerelement beispielsweise Parameter enthält, können Sie die Parameterwerte überprüfen, die Security Hub CSPM derzeit bei der Durchführung von Sicherheitsprüfungen für das Steuerelement verwendet.

Registerkarte „Ressourcen“

Auf dieser Registerkarte finden Sie Einzelheiten zu den Ressourcen, die an einem Befund beteiligt waren. Wenn Sie bei dem Konto angemeldet sind, dem eine Ressource gehört, können Sie die Ressource in der entsprechenden AWS-Service Konsole überprüfen. Wenn Sie nicht der Besitzer einer Ressource sind, wird auf dieser Registerkarte die AWS-Konto ID des Besitzers angezeigt.

In der Zeile „Details“ werden ressourcenspezifische Details zu einem Ergebnis angezeigt. Sie zeigt den [ResourceDetails](#) Abschnitt des Ergebnisses im JSON-Format.

In der Zeile „Tags“ werden Tag-Schlüssel und -Werte angezeigt, die den Ressourcen zugewiesen sind, die an einem Befund beteiligt sind. Ressourcen, die [vom GetResources Betrieb der AWS Resource Groups Tagging-API unterstützt](#) werden, können markiert werden. Security Hub CSPM

ruft diesen Vorgang bei der Verarbeitung neuer oder aktualisierter Ergebnisse mithilfe einer [serviceverknüpften Rolle](#) auf und ruft die Ressourcen-Tags ab, wenn das Resource . Id Feld AWS Security Finding Format (ASFF) mit dem ARN einer Ressource gefüllt ist. Security Hub CSPM ignoriert ungültige Ressourcen. IDs Weitere Informationen zur Aufnahme von Ressourcen-Tags in die Ergebnisse finden Sie unter. [Tags](#)

Registerkarte „Verlauf“

Auf dieser Registerkarte wird der Verlauf eines Befundes nachverfolgt. Die Fundhistorie ist für aktive und archivierte Ergebnisse verfügbar. Es bietet eine unveränderliche Aufzeichnung der Änderungen, die im Laufe der Zeit an einem Ergebnis vorgenommen wurden, einschließlich der Änderung, welches ASFF-Feld geändert wurde, wann die Änderung vorgenommen wurde und von welchem Benutzer. Auf jeder Seite der Registerkarte werden bis zu 20 Änderungen angezeigt. Neuere Änderungen werden zuerst angezeigt.

Bei aktiven Ergebnissen steht die Fundhistorie für bis zu 90 Tage zur Verfügung. Für archivierte Ergebnisse ist die Fundhistorie für bis zu 30 Tage verfügbar. Der Suchverlauf umfasst Änderungen, die manuell oder automatisch durch die [CSPM-Automatisierungsregeln von Security Hub](#) vorgenommen wurden. Änderungen an Zeitstempelfeldern der obersten Ebene, wie z. B. den Feldern und, sind nicht enthalten. CreatedAt UpdatedAt

Wenn Sie mit einem Security Hub CSPM-Administratorkonto angemeldet sind, bezieht sich der Suchverlauf auf das Administratorkonto und alle Mitgliedskonten.

Registerkarte „Bedrohung“

Diese Registerkarte enthält Daten aus den [ActionMalware](#), und [ProcessDetails](#)Objekten der ASFF, einschließlich der Art der Bedrohung und ob es sich bei einer Ressource um das Ziel oder den Akteur handelt. Diese Angaben gelten in der Regel für Ergebnisse, die ihren Ursprung in Amazon haben GuardDuty.

Registerkarte Sicherheitslücken

Auf dieser Registerkarte werden Daten aus dem [Vulnerability](#)Objekt des ASFF angezeigt, einschließlich Informationen darüber, ob es im Zusammenhang mit einem Befund Exploits oder verfügbare Fixes gibt. Diese Angaben gelten in der Regel für Ergebnisse, die ihren Ursprung in Amazon Inspector haben.

Die Zeilen auf jeder Registerkarte enthalten eine Kopier- oder Filteroption. Wenn Sie beispielsweise den Bereich für ein Ergebnis öffnen, das den Workflow-Status Benachrichtigt hat, können Sie die Filteroption neben der Zeile Workflow-Status auswählen. Wenn Sie Alle Ergebnisse mit diesem

Wert anzeigen wählen, filtert Security Hub CSPM die Ergebnistabelle und zeigt nur Ergebnisse mit demselben Workflow-Status an.

Details und Verlauf der Ergebnisse überprüfen

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um die Suchdetails in Security Hub CSPM zu überprüfen.

Wenn Sie die regionsübergreifende Aggregation aktivieren und sich bei der Aggregationsregion anmelden, umfasst die Suche nach Daten auch Daten aus der Aggregationsregion und verknüpften Regionen. In anderen Regionen ist das Suchen von Daten nur für diese Region spezifisch. Weitere Informationen zur regionsübergreifenden Aggregation finden Sie unter. [Aggregation von CSPM-Daten über Regionen hinweg](#)

Security Hub CSPM console

Einzelheiten und Verlauf der Ergebnisse überprüfen

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>
2. Gehen Sie wie folgt vor, um eine Ergebnisliste anzuzeigen:
 - Wählen Sie im Navigationsbereich Findings aus. Fügen Sie nach Bedarf Suchfilter hinzu, um die Ergebnisliste einzugrenzen.
 - Wählen Sie im Navigationsbereich Insights aus. Wählen Sie einen Einblick. Wählen Sie dann in der Ergebnisliste ein Insight-Ergebnis aus.
 - Wählen Sie im Navigationsbereich Integrationen aus. Wählen Sie Ergebnisse anzeigen für eine Integration aus.
 - Wählen Sie im Navigationsbereich Controls aus.
3. Wählen Sie ein Ergebnis aus. Im Ergebnisfenster werden die Details des Ergebnisses angezeigt.
4. Führen Sie im Ergebnisfenster einen der folgenden Schritte aus:
 - Wählen Sie eine Registerkarte, um spezifische Details zum Ergebnis zu überprüfen.
 - Um Maßnahmen gegen das Ergebnis zu ergreifen, wählen Sie eine Option aus dem Menü „Aktionen“ aus.
 - Um den Befund in Amazon Detective zu untersuchen, wählen Sie eine Option Untersuchen.

Note

Wenn Sie sich mit einem Mitgliedskonto integrieren AWS Organizations und dort angemeldet sind, enthält das Ergebnisfenster den Kontonamen. Für Mitgliedskonten, die manuell statt über Organizations eingeladen werden, enthält das Suchfeld nur die Konto-ID.

Security Hub CSPM API

Verwenden Sie den [GetFindings](#) Betrieb der Security Hub CSPM-API, oder wenn Sie die verwenden AWS CLI, führen Sie den Befehl aus. [get-findings](#) Sie können einen oder mehrere Werte für den `Filters` Parameter angeben, um die abzurufenden Ergebnisse einzugrenzen.

Wenn das Volumen der Ergebnisse zu groß ist, können Sie den `MaxResults` Parameter verwenden, um die Ergebnisse auf eine bestimmte Zahl zu beschränken, und den `NextToken` Parameter, um die Ergebnisse zu paginieren. Verwenden Sie den `SortCriteria` Parameter, um die Ergebnisse nach einem bestimmten Feld zu sortieren.

Mit dem folgenden AWS CLI Befehl werden beispielsweise die Ergebnisse abgerufen, die den angegebenen Filterkriterien entsprechen, und die Ergebnisse werden in absteigender Reihenfolge nach dem `LastObservedAt` Feld sortiert. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (`\`) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub get-findings \
--filters '{"GeneratorId":[{"Value": "aws-  
foundational", "Comparison": "PREFIX"}], "WorkflowStatus": [{"Value":  
"NEW", "Comparison": "EQUALS"}], "Confidence": [{"Gte": 85}]}' --sort-criteria  
'{"Field": "LastObservedAt", "SortOrder": "desc"}' --page-size 5 --max-items 100
```

Verwenden Sie den Vorgang, um den Verlauf der [GetFindingHistory](#) Ergebnisse zu überprüfen. Wenn Sie den verwenden AWS CLI, führen Sie den [get-finding-history](#) Befehl aus. Identifizieren Sie das Ergebnis, für das Sie den Verlauf abrufen möchten, mit den `Id` Feldern `ProductArn` und. Informationen zu diesen Feldern finden Sie unter [AwsSecurityFindingIdentifier](#). Jede Anfrage kann den Verlauf für nur einen Befund abrufen.

Mit dem folgenden AWS CLI Befehl wird beispielsweise der Verlauf für den angegebenen Befund abgerufen. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (`\`) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub get-finding-history \  
--region us-west-2 \  
--finding-identifier Id="a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",ProductArn="arn:aws:securityhub:us-west-2:123456789012:product/123456789012/default" \  
--max-results 2 \  
--start-time "2021-09-30T15:53:35.573Z" \  
--end-time "2021-09-31T15:53:35.573Z"
```

PowerShell

Verwenden Sie das Get-SHUBFinding Cmdlet. Füllen Sie optional den Filter Parameter aus, um die abzurufenden Ergebnisse einzugrenzen.

Das folgende Cmdlet ruft beispielsweise die Ergebnisse ab, die den angegebenen Filtern entsprechen.

```
Get-SHUBFinding -Filter @{AwsAccountId =  
[Amazon.SecurityHub.Model.StringFilter]@{Comparison = "EQUALS"; Value =  
"XXX"};ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{Comparison =  
"EQUALS"; Value = 'FAILED'}}
```

Note

Wenn Sie Ergebnisse nach CompanyName oder filternProductName, verwendet Security Hub CSPM die Werte, die Teil des ProductFields ASFF-Objekts sind. Security Hub CSPM verwendet die Felder und auf oberster Ebene CompanyName nicht. ProductName

Ergebnisse im Security Hub CSPM filtern

AWS Security Hub Cloud Security Posture Management (CSPM) generiert seine eigenen Ergebnisse aus Sicherheitsprüfungen und erhält Ergebnisse aus integrierten Produkten. Sie können eine Liste der Ergebnisse auf den Seiten Findings, Integrations und Insights der Security Hub CSPM-Konsole anzeigen. Sie können Filter hinzufügen, um eine Ergebnisliste einzugrenzen, sodass die Liste für Ihre Organisation oder Ihren Anwendungsfall relevant ist.

Informationen zum Filtern von Ergebnissen für eine bestimmte Sicherheitskontrolle finden Sie unter [the section called “Filterung und Sortierung der Kontrollergebnisse”](#). Die Informationen auf dieser Seite gelten für die Seiten Ergebnisse, Einblicke und Integrationen.

Standardfilter für Suchlisten

Standardmäßig werden Suchlisten auf der Security Hub CSPM-Konsole anhand der `Workflow.Status` Felder `RecordState` und des AWS Security Finding Formats (ASFF) gefiltert. Dies gilt zusätzlich zu den Filtern für einen bestimmten Einblick oder eine bestimmte Integration.

Der Datensatzstatus gibt an, ob ein Ergebnis aktiv oder archiviert ist. Standardmäßig werden in einer Ergebnisliste nur aktive Ergebnisse angezeigt. Ein Anbieter von Ergebnissen kann ein Ergebnis archivieren, wenn es nicht mehr aktiv oder wichtig ist. Security Hub CSPM archiviert Kontrollergebnisse auch automatisch, wenn die zugehörige Ressource gelöscht wird.

Der Workflow-Status gibt den Status einer Untersuchung eines Ergebnisses an. Standardmäßig werden in einer Ergebnisliste nur Ergebnisse mit dem Workflow-Status `NEW` oder `NOTIFIED` angezeigt. Sie können den Workflow-Status eines Ergebnisses aktualisieren.

Anweisungen zum Hinzufügen von Filtern

Sie können eine Ergebnisliste nach bis zu zehn Attributen filtern. Für jedes Attribut können Sie bis zu 20 Filterwerte angeben.

Beim Filtern der Ergebnisliste wendet Security Hub CSPM AND Logik auf den Filtersatz an. Ein Ergebnis stimmt nur dann überein, wenn es allen bereitgestellten Filtern entspricht. Wenn Sie beispielsweise GuardDuty als Filter für den Produktnamen und AwsS3Bucket als Filter für den Ressourcentyp hinzufügen, zeigt Security Hub CSPM Ergebnisse an, die diesen beiden Kriterien entsprechen.

Security Hub CSPM wendet OR Logik auf Filter an, die dasselbe Attribut, aber unterschiedliche Werte verwenden. Wenn Sie beispielsweise GuardDuty sowohl als auch Amazon Inspector als Filterwerte für den Produktnamen hinzufügen, zeigt Security Hub CSPM Ergebnisse an, die entweder von Amazon Inspector GuardDuty oder Amazon Inspector generiert wurden.

Um Filter zu einer Ergebnisliste hinzuzufügen (Konsole)

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>

2. Um eine Ergebnisliste anzuzeigen, führen Sie im Navigationsbereich eine der folgenden Aktionen aus:
 - Wählen Sie Ergebnisse aus.
 - Wählen Sie Insights. Wählen Sie einen Einblick. Wählen Sie dann in der Ergebnisliste ein Insight-Ergebnis aus.
 - Wählen Sie Integrations (Integrationen) aus. Wählen Sie Ergebnisse anzeigen für eine Integration aus.
3. Wählen Sie im Feld Filter hinzufügen ein oder mehrere Felder aus, nach denen gefiltert werden soll.

Wenn Sie nach Firmenname oder Produktname filtern, verwendet die Konsole die `ProductName` Felder der obersten Ebene `CompanyName` und das AWS Security Finding Format (ASFF). Die API verwendet die Werte, die unter verschachtelt sind. `ProductFields`

4. Wählen Sie den Filterübereinstimmungstyp aus.

Für einen Zeichenkettenfilter können Sie aus den folgenden Optionen wählen:

- `ist` — Findet einen Wert, der genau dem Filterwert entspricht.
- `beginnt mit` — Findet einen Wert, der mit dem Filterwert beginnt.
- `ist nicht` — Findet einen Wert, der nicht mit dem Filterwert übereinstimmt.
- `beginnt nicht mit` — Findet einen Wert, der nicht mit dem Filterwert beginnt.

Für das Feld Ressourcen-Tags können Sie nach bestimmten Schlüsseln oder Werten filtern.

Für einen numerischen Filter können Sie wählen, ob Sie eine einzelne Zahl (Simple) oder einen Zahlenbereich (Range) angeben möchten.

Für einen Datums- oder Uhrzeitfilter können Sie wählen, ob Sie eine Zeitspanne vom aktuellen Datum und der aktuellen Uhrzeit (Rollendes Fenster) oder einen bestimmten Datumsbereich (fester Bereich) angeben möchten.

Das Hinzufügen mehrerer Filter hat die folgenden Interaktionen:

- `ist` und `beginnt mit` Filtern werden durch OR verknüpft. Ein Wert stimmt überein, wenn er einen der Filterwerte enthält. Wenn Sie beispielsweise die Bezeichnung Schweregrad auf KRITISCH

und die Bezeichnung Schweregrad auf HOCH angeben, enthalten die Ergebnisse sowohl kritische als auch Ergebnisse mit hohem Schweregrad.

- ist nicht und beginnt auch nicht mit Filtern, die durch UND verknüpft werden. Ein Wert stimmt nur überein, wenn er keinen dieser Filterwerte enthält. Wenn Sie beispielsweise angeben, dass die Bezeichnung Schweregrad nicht NIEDRIG und die Bezeichnung Schweregrad nicht MITTEL ist, enthalten die Ergebnisse keine Ergebnisse mit niedrigem oder mittlerem Schweregrad.

Wenn Sie einen Is-Filter für ein Feld verwenden, können Sie nicht den Filter Ist nicht oder A fängt nicht mit an für dasselbe Feld verwenden.

5. Geben Sie den Filterwert an. Bei Zeichenkettenfiltern unterscheidet der Filterwert zwischen Groß- und Kleinschreibung.
6. Wählen Sie Anwenden aus.

Für einen vorhandenen Filter können Sie den Übereinstimmungstyp oder den Wert des Filters ändern. Wählen Sie in einer gefilterten Ergebnisliste den Filter aus. Wählen Sie im Feld Filter bearbeiten den neuen Treffertyp oder Wert aus, und klicken Sie dann auf Anwenden.

Um einen Filter zu entfernen, wählen Sie das X-Symbol. Die Liste wird automatisch aktualisiert, um die Änderung widerzuspiegeln.

Gruppierung der Ergebnisse in Security Hub CSPM

Sie können Ergebnisse in AWS Security Hub Cloud Security Posture Management (CSPM) auf der Grundlage der Werte eines ausgewählten Attributs gruppieren.

Wenn Sie die Ergebnisse gruppieren, wird die Ergebnisliste durch eine Werteliste für das ausgewählte Attribut in den entsprechenden Ergebnissen ersetzt. Für jeden Wert wird in der Liste die Anzahl der übereinstimmenden Ergebnisse angezeigt.

Wenn Sie die Ergebnisse beispielsweise nach AWS-Konto ID gruppieren, wird eine Liste von Konto-IDs mit der Anzahl der übereinstimmenden Ergebnisse für jedes Konto angezeigt.

Security Hub CSPM kann bis zu 100 Werte für ein ausgewähltes Attribut anzeigen. Wenn es mehr als 100 Werte gibt, werden nur die ersten 100 angezeigt.

Wenn Sie einen Attributwert auswählen, zeigt Security Hub CSPM die Liste der passenden Ergebnisse für diesen Wert an.

Um die Ergebnisse in einer Ergebnisliste zu gruppieren (Konsole)

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>
2. Um eine Ergebnisliste anzuzeigen, führen Sie im Navigationsbereich eine der folgenden Aktionen aus:
 - Wählen Sie Ergebnisse aus.
 - Wählen Sie Insights. Wählen Sie einen Einblick. Wählen Sie dann in der Ergebnisliste ein Insight-Ergebnis aus.
 - Wählen Sie Integrations (Integrationen) aus. Wählen Sie Ergebnisse anzeigen für eine Integration aus.
3. Wählen Sie in der Dropdownliste Gruppieren nach das Attribut aus, das für die Gruppierung verwendet werden soll.

Um ein Gruppierungsattribut zu entfernen, wählen Sie das X-Symbol. Wenn Sie das Gruppierungsattribut entfernen, ändert sich die Liste von der Liste der Attributwerte in eine Ergebnisliste.

Den Workflow-Status von Ergebnissen in Security Hub CSPM festlegen

Der Workflow-Status verfolgt den Fortschritt Ihrer Untersuchung zu einem Ergebnis. Der Workflow-Status ist spezifisch für ein einzelnes Ergebnis und hat keinen Einfluss auf die Generierung neuer Ergebnisse. Wenn Sie beispielsweise den Workflow-Status eines Ergebnisses auf SUPPRESSED oder ändernRESOLVED, verhindert Ihre Änderung nicht, dass Security Hub CSPM ein neues Ergebnis für dasselbe Problem generiert.

Der Workflow-Status eines Befundes kann einer der folgenden Werte sein.

NEU

Der Ausgangszustand eines Ergebnisses, bevor Sie es überprüfen.

Ergebnisse, die aus integrierten Quellen aufgenommen wurden AWS-Services AWS Config, haben z. B. ihren ursprünglichen Status.

Security Hub CSPM setzt in den folgenden Fällen auch den Workflow-Status von entweder NOTIFIED oder RESOLVED NEW auf zurück:

- RecordState ändert sich von ARCHIVED in ACTIVE.
- Compliance.Status ändert sich von PASSED zu FAILED, WARNING oder NOT_AVAILABLE

Diese Änderungen bedeuten, dass zusätzliche Untersuchungen erforderlich sind.

BENACHRICHTIGT

Gibt an, dass Sie den Ressourceneigentümer über das Sicherheitsproblem informiert haben. Sie können diesen Status verwenden, wenn Sie nicht der Ressourceneigentümer sind und einen Eingriff von diesem benötigen, um ein Sicherheitsproblem zu beheben.

Wenn einer der folgenden Fälle eintritt, wird der Workflow-Status automatisch von NOTIFIED zu geändert NEW:

- RecordState ändert sich von ARCHIVED in ACTIVE.
- Compliance.Status ändert sich von PASSED zu FAILED WARNING, oder NOT_AVAILABLE.

UNTERDRÜCKT

Zeigt an, dass Sie das Ergebnis überprüft haben und nicht der Meinung sind, dass weitere Maßnahmen erforderlich sind.

Der Workflow-Status eines SUPPRESSED Ergebnisses RecordState ändert sich nicht, wenn er von ARCHIVED zu geändert wird ACTIVE.

GELÖST

Das Ergebnis wurde überprüft und korrigiert und gilt nun als gelöst.

Das Ergebnis bleibt bestehen RESOLVED, sofern nicht einer der folgenden Fälle eintritt:

- RecordState ändert sich von ARCHIVED in ACTIVE.
- Compliance.Status ändert sich von PASSED zu FAILED WARNING, oder NOT_AVAILABLE.

In diesen Fällen wird der Workflow-Status automatisch auf zurückgesetzt NEW.

Falls dies der Fall Compliance.Status ist PASSED, setzt Security Hub CSPM den Workflow-Status automatisch auf RESOLVED

Den Workflow-Status von Ergebnissen festlegen

Um den Workflow-Status eines oder mehrerer Ergebnisse zu ändern, können Sie die Security Hub CSPM-Konsole oder die Security Hub CSPM-API verwenden. Wenn Sie den Workflow-Status eines Befundes ändern, beachten Sie, dass es mehrere Minuten dauern kann, bis Security Hub CSPM Ihre Anfrage bearbeitet und das Ergebnis aktualisiert hat.

Tip

Sie können den Workflow-Status von Ergebnissen auch automatisch ändern, indem Sie Automatisierungsregeln verwenden. Mit Automatisierungsregeln konfigurieren Sie Security Hub CSPM so, dass der Workflow-Status von Ergebnissen auf der Grundlage der von Ihnen angegebenen Kriterien automatisch aktualisiert wird. Weitere Informationen finden Sie unter [Grundlegendes zu den Automatisierungsregeln in Security Hub CSPM](#).

Um den Workflow-Status eines oder mehrerer Ergebnisse zu ändern, wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten.

Security Hub CSPM console

Um den Workflow-Status von Ergebnissen zu ändern

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>
2. Führen Sie im Navigationsbereich einen der folgenden Schritte aus, um eine Tabelle mit Ergebnissen anzuzeigen:
 - Wählen Sie Ergebnisse aus.
 - Wählen Sie Insights. Wählen Sie dann einen Einblick aus. Wählen Sie in den Insight-Ergebnissen ein Ergebnis aus.
 - Wählen Sie Integrations (Integrationen) aus. Wählen Sie dann im Abschnitt für die Integration die Option Ergebnisse anzeigen aus.
 - Wählen Sie Sicherheitsstandards aus. Wählen Sie dann im Abschnitt für den Standard die Option Ergebnisse anzeigen aus. Wählen Sie in der Kontrolltabelle ein Steuerelement aus, um die Ergebnisse für das Steuerelement anzuzeigen.
3. Aktivieren Sie in der Tabelle mit den Ergebnissen das Kontrollkästchen für jedes Ergebnis, dessen Workflow-Status Sie ändern möchten.

4. Wählen Sie oben auf der Seite Workflow-Status und dann den neuen Workflow-Status für die ausgewählten Ergebnisse aus.
5. Geben Sie im Dialogfeld Workflow-Status festlegen optional eine Notiz ein, in der der Grund für die Änderung des Workflow-Status detailliert beschrieben wird. Wählen Sie dann Status festlegen aus.

Security Hub CSPM API

Verwenden Sie die [BatchUpdateFindings](#) Operation. Geben Sie sowohl die Ergebnis-ID als auch den ARN des Produkts an, das den Befund generiert hat. Sie können diese Details mithilfe der [GetFindings](#) Operation abrufen.

AWS CLI

Führen Sie den Befehl [batch-update-findings](#) aus. Geben Sie sowohl die Ergebnis-ID als auch den ARN des Produkts an, das den Befund generiert hat. Sie können diese Details abrufen, indem Sie den Befehl [get-findings](#) ausführen.

```
batch-update-findings --finding-identifiers  
Id="<findingID>",ProductArn="<productARN>" --workflow Status="<workflowStatus>"
```

Beispiel

```
aws securityhub batch-update-findings --finding-identifiers  
Id="arn:aws:securityhub:us-west-1:123456789012:subscription/  
pci-dss/v/3.2.1/PCI.Lambda.2/finding/a1b2c3d4-5678-90ab-cdef-  
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-west-1::product/aws/securityhub" --  
workflow Status="RESOLVED"
```

Ergebnisse an eine benutzerdefinierte Security Hub CSPM-Aktion senden

Sie können benutzerdefinierte AWS Security Hub Cloud Security Posture Management (CSPM) -Aktionen erstellen, um Security Hub CSPM mit Amazon zu automatisieren. EventBridge Für benutzerdefinierte Aktionen lautet der Ereignistyp Security Hub Findings - Custom Action. Nachdem Sie eine benutzerdefinierte Aktion eingerichtet haben, können Sie Ergebnisse an sie senden. Weitere Informationen und detaillierte Schritte zum Erstellen benutzerdefinierter Aktionen finden Sie unter [the section called “Automatisierte Reaktion und Problembehebung”](#).

Um Ergebnisse an eine benutzerdefinierte Aktion (Konsole) zu senden

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>
2. Gehen Sie wie folgt vor, um eine Ergebnisliste anzuzeigen:
 - Wählen Sie im Security Hub CSPM-Navigationsbereich Findings aus.
 - Wählen Sie im Security Hub CSPM-Navigationsbereich Insights aus. Wählen Sie einen Einblick aus. Wählen Sie dann in der Ergebnisliste ein Insight-Ergebnis aus.
 - Wählen Sie im Security Hub CSPM-Navigationsbereich Integrationen aus. Wählen Sie Ergebnisse für eine Integration anzeigen aus.
 - Wählen Sie im Security Hub CSPM-Navigationsbereich die Option Sicherheitsstandards aus. Wählen Sie Ergebnisse anzeigen, um eine Liste mit Kontrollen anzuzeigen. Wählen Sie dann den Namen des Steuerelements.
3. Aktivieren Sie in der Ergebnisliste das Kontrollkästchen für jedes Ergebnis, das an die benutzerdefinierte Aktion gesendet werden soll.

Sie können bis zu 20 Ergebnisse gleichzeitig senden.

4. Wählen Sie für Aktionen die benutzerdefinierte Aktion aus.

AWS Format für Sicherheitssuche (ASFF)

AWS Security Hub Cloud Security Posture Management (CSPM) nutzt und aggregiert Ergebnisse aus integrierten AWS-Services Produkten und Produkten von Drittanbietern. Security Hub CSPM verarbeitet diese Ergebnisse mithilfe eines Standardformats für Ergebnisse, dem AWS Security Finding Format (ASFF), das zeitaufwändige Datenkonvertierungen überflüssig macht.

Diese Seite bietet einen vollständigen Überblick über die JSON-Daten für ein Ergebnis im AWS Security Finding Format (ASFF). Das Format leitet sich vom [JSON-Schema](#) ab. Wählen Sie den Namen eines verknüpften Objekts, um ein Beispiel für ein Ergebnis für dieses Objekt zu überprüfen. Der Vergleich Ihrer Security Hub CSPM-Ergebnisse mit den hier aufgeführten Ressourcen und Beispielen kann Ihnen bei der Interpretation Ihrer Ergebnisse helfen.

Eine Beschreibung der einzelnen ASFF-Attribute finden Sie unter und [the section called “Erforderliche ASFF-Attribute der obersten Ebene”](#) [the section called “Optionale ASFF-Attribute der obersten Ebene”](#)

```

"Findings": [
  {
    "Action": {
      "ActionType": "string",
      "AwsApiCallAction": {
        "AffectedResources": {
          "string": "string"
        },
        "Api": "string",
        "CallerType": "string",
        "DomainDetails": {
          "Domain": "string"
        },
        "FirstSeen": "string",
        "LastSeen": "string",
        "RemoteIpDetails": {
          "City": {
            "CityName": "string"
          },
          "Country": {
            "CountryCode": "string",
            "CountryName": "string"
          },
          "IpAddressV4": "string",
          "Geolocation": {
            "Lat": number,
            "Lon": number
          },
          "Organization": {
            "Asn": number,
            "AsnOrg": "string",
            "Isp": "string",
            "Org": "string"
          }
        },
        "ServiceName": "string"
      },
      "DnsRequestAction": {
        "Blocked": boolean,
        "Domain": "string",
        "Protocol": "string"
      },
      "NetworkConnectionAction": {

```

```
"Blocked": boolean,
"ConnectionDirection": "string",
"LocalPortDetails": {
  "Port": number,
  "PortName": "string"
},
"Protocol": "string",
"RemoteIpDetails": {
  "City": {
    "CityName": "string"
  },
  "Country": {
    "CountryCode": "string",
    "CountryName": "string"
  },
  "IpAddressV4": "string",
  "Geolocation": {
    "Lat": number,
    "Lon": number
  },
  "Organization": {
    "Asn": number,
    "AsnOrg": "string",
    "Isp": "string",
    "Org": "string"
  }
},
"RemotePortDetails": {
  "Port": number,
  "PortName": "string"
}
},
"PortProbeAction": {
  "Blocked": boolean,
  "PortProbeDetails": [{
    "LocalIpDetails": {
      "IpAddressV4": "string"
    },
    "LocalPortDetails": {
      "Port": number,
      "PortName": "string"
    },
    "RemoteIpDetails": {
      "City": {
```

```

    "CityName": "string"
  },
  "Country": {
    "CountryCode": "string",
    "CountryName": "string"
  },
  "GeoLocation": {
    "Lat": number,
    "Lon": number
  },
  "IpAddressV4": "string",
  "Organization": {
    "Asn": number,
    "AsnOrg": "string",
    "Isp": "string",
    "Org": "string"
  }
}
]]
}
},
"AwsAccountId": "string",
"AwsAccountName": "string",
"CompanyName": "string",
"Compliance": {
  "AssociatedStandards": [{
    "StandardsId": "string"
  }],
  "RelatedRequirements": ["string"],
  "SecurityControlId": "string",
  "SecurityControlParameters": [
    {
      "Name": "string",
      "Value": ["string"]
    }
  ],
  "Status": "string",
  "StatusReasons": [
    {
      "Description": "string",
      "ReasonCode": "string"
    }
  ]
},

```

```
"Confidence": number,
"CreatedAt": "string",
"Criticality": number,
"Description": "string",
"Detection": {
  "Sequence": {
    "Uid": "string",
    "Actors": [{
      "Id": "string",
      "Session": {
        "Uid": "string",
        "MfaStatus": "string",
        "CreatedTime": "string",
        "Issuer": "string"
      },
      "User": {
        "CredentialUid": "string",
        "Name": "string",
        "Type": "string",
        "Uid": "string",
        "Account": {
          "Uid": "string",
          "Name": "string"
        }
      }
    }
  ],
  "Endpoints": [{
    "Id": "string",
    "Ip": "string",
    "Domain": "string",
    "Port": number,
    "Location": {
      "City": "string",
      "Country": "string",
      "Lat": number,
      "Lon": number
    }
  ],
  "AutonomousSystem": {
    "Name": "string",
    "Number": number
  },
  "Connection": {
    "Direction": "string"
  }
}
```



```

    ]],
    "Signals": [{
      "Id": "string",
      "Title": "string",
      "ActorIds": ["string"],
      "Count": number,
      "FirstSeenAt": number,
      "SignalIndicators": [
        {
          "Key": "string",
          "Title": "string",
          "Values": ["string"]
        },
        {
          "Key": "string",
          "Title": "string",
          "Values": ["string"]
        }
      ],
      "LastSeenAt": number,
      "Name": "string",
      "ResourceIds": ["string"],
      "Type": "string"
    }],
    "SequenceIndicators": [
      {
        "Key": "string",
        "Title": "string",
        "Values": ["string"]
      },
      {
        "Key": "string",
        "Title": "string",
        "Values": ["string"]
      }
    ]
  },
  "FindingProviderFields": {
    "Confidence": number,
    "Criticality": number,
    "RelatedFindings": [{
      "ProductArn": "string",
      "Id": "string"
    }
  ]
}

```

```
    ]],
    "Severity": {
      "Label": "string",
      "Normalized": number,
      "Original": "string"
    },
    "Types": ["string"]
  },
  "FirstObservedAt": "string",
  "GeneratorId": "string",
  "Id": "string",
  "LastObservedAt": "string",
  "Malware": [{
    "Name": "string",
    "Path": "string",
    "State": "string",
    "Type": "string"
  }],
  "Network": {
    "DestinationDomain": "string",
    "DestinationIPv4": "string",
    "DestinationIPv6": "string",
    "DestinationPort": number,
    "Direction": "string",
    "OpenPortRange": {
      "Begin": integer,
      "End": integer
    },
    "Protocol": "string",
    "SourceDomain": "string",
    "SourceIPv4": "string",
    "SourceIPv6": "string",
    "SourceMac": "string",
    "SourcePort": number
  },
  "NetworkPath": [{
    "ComponentId": "string",
    "ComponentType": "string",
    "Egress": {
      "Destination": {
        "Address": ["string"],
        "PortRanges": [{
          "Begin": integer,
          "End": integer
```

```

    ]]
  },
  "Protocol": "string",
  "Source": {
    "Address": ["string"],
    "PortRanges": [{
      "Begin": integer,
      "End": integer
    }]
  }
},
  "Ingress": {
    "Destination": {
      "Address": ["string"],
      "PortRanges": [{
        "Begin": integer,
        "End": integer
      }]
    }
  },
  "Protocol": "string",
  "Source": {
    "Address": ["string"],
    "PortRanges": [{
      "Begin": integer,
      "End": integer
    }]
  }
}
}],
  "Note": {
    "Text": "string",
    "UpdatedAt": "string",
    "UpdatedBy": "string"
  },
  "PatchSummary": {
    "FailedCount": number,
    "Id": "string",
    "InstalledCount": number,
    "InstalledOtherCount": number,
    "InstalledPendingReboot": number,
    "InstalledRejectedCount": number,
    "MissingCount": number,
    "Operation": "string",
    "OperationEndTime": "string",

```

```

    "OperationStartTime": "string",
    "RebootOption": "string"
  },
  "Process": {
    "LaunchedAt": "string",
    "Name": "string",
    "ParentPid": number,
    "Path": "string",
    "Pid": number,
    "TerminatedAt": "string"
  },
  "ProductArn": "string",
  "ProductFields": {
    "string": "string"
  },
  "ProductName": "string",
  "RecordState": "string",
  "Region": "string",
  "RelatedFindings": [{
    "Id": "string",
    "ProductArn": "string"
  }],
  "Remediation": {
    "Recommendation": {
      "Text": "string",
      "Url": "string"
    }
  },
  "Resources": [{
    "ApplicationArn": "string",
    "ApplicationName": "string",
    "DataClassification": {
      "DetailedResultsLocation": "string",
      "Result": {
        "AdditionalOccurrences": boolean,
        "CustomDataIdentifiers": {
          "Detections": [{
            "Arn": "string",
            "Count": integer,
            "Name": "string",
            "Occurrences": {
              "Cells": [{
                "CellReference": "string",
                "Column": integer,

```

```
    "ColumnName": "string",
    "Row": integer
  }],
  "LineRanges": [{
    "End": integer,
    "Start": integer,
    "StartColumn": integer
  }],
  "OffsetRanges": [{
    "End": integer,
    "Start": integer,
    "StartColumn": integer
  }],
  "Pages": [{
    "LineRange": {
      "End": integer,
      "Start": integer,
      "StartColumn": integer
    },
    "OffsetRange": {
      "End": integer,
      "Start": integer,
      "StartColumn": integer
    },
    "PageNumber": integer
  }],
  "Records": [{
    "JsonPath": "string",
    "RecordIndex": integer
  }]
}
}],
"TotalCount": integer
},
"MimeType": "string",
"SensitiveData": [{
  "Category": "string",
  "Detections": [{
    "Count": integer,
    "Occurrences": {
      "Cells": [{
        "CellReference": "string",
        "Column": integer,
        "ColumnName": "string",
```

```

    "Row": integer
  }],
  "LineRanges": [{
    "End": integer,
    "Start": integer,
    "StartColumn": integer
  }],
  "OffsetRanges": [{
    "End": integer,
    "Start": integer,
    "StartColumn": integer
  }],
  "Pages": [{
    "LineRange": {
      "End": integer,
      "Start": integer,
      "StartColumn": integer
    },
    "OffsetRange": {
      "End": integer,
      "Start": integer,
      "StartColumn": integer
    },
    "PageNumber": integer
  }],
  "Records": [{
    "JsonPath": "string",
    "RecordIndex": integer
  }]
},
"Type": "string"
}],
"TotalCount": integer
}],
"SizeClassified": integer,
"Status": {
  "Code": "string",
  "Reason": "string"
}
},
"Details": {
  "AwsAmazonMQBroker": {
    "AutoMinorVersionUpgrade": boolean,

```

```

    "BrokerArn": "string",
    "BrokerId": "string",
    "BrokerName": "string",
    "Configuration": {
        "Id": "string",
        "Revision": integer
    },
    "DeploymentMode": "string",
    "EncryptionOptions": {
        "UseAwsOwnedKey": boolean
    },
    "EngineType": "string",
    "EngineVersion": "string",
    "HostInstanceType": "string",
    "Logs": {
        "Audit": boolean,
        "AuditLogGroup": "string",
        "General": boolean,
        "GeneralLogGroup": "string"
    },
    "MaintenanceWindowStartTime": {
        "DayOfWeek": "string",
        "TimeOfDay": "string",
        "TimeZone": "string"
    },
    "PubliclyAccessible": boolean,
    "SecurityGroups": [
        "string"
    ],
    "StorageType": "string",
    "SubnetIds": [
        "string",
        "string"
    ],
    "Users": [{
        "Username": "string"
    }]
},
"AwsApiGatewayRestApi": {
    "ApiKeySource": "string",
    "BinaryMediaTypes": [" string"],
    "CreatedDate": "string",
    "Description": "string",
    "EndpointConfiguration": {

```

```

    "Types": ["string"]
  },
  "Id": "string",
  "MinimumCompressionSize": number,
  "Name": "string",
  "Version": "string"
},
"AwsApiGatewayStage": {
  "AccessLogSettings": {
    "DestinationArn": "string",
    "Format": "string"
  },
  "CacheClusterEnabled": boolean,
  "CacheClusterSize": "string",
  "CacheClusterStatus": "string",
  "CanarySettings": {
    "DeploymentId": "string",
    "PercentTraffic": number,
    "StageVariableOverrides": [{
      "string": "string"
    }],
    "UseStageCache": boolean
  },
  "ClientCertificateId": "string",
  "CreatedDate": "string",
  "DeploymentId": "string",
  "Description": "string",
  "DocumentationVersion": "string",
  "LastUpdatedDate": "string",
  "MethodSettings": [{
    "CacheDataEncrypted": boolean,
    "CachingEnabled": boolean,
    "CacheTtlInSeconds": number,
    "DataTraceEnabled": boolean,
    "HttpMethod": "string",
    "LoggingLevel": "string",
    "MetricsEnabled": boolean,
    "RequireAuthorizationForCacheControl": boolean,
    "ResourcePath": "string",
    "ThrottlingBurstLimit": number,
    "ThrottlingRateLimit": number,
    "UnauthorizedCacheControlHeaderStrategy": "string"
  }],
  "StageName": "string",

```



```
"TracingEnabled": boolean,
"Variables": {
  "string": "string"
},
"WebAclArn": "string"
},
"AwsApiGatewayV2Api": {
  "ApiEndpoint": "string",
  "ApiId": "string",
  "ApiKeySelectionExpression": "string",
  "CorsConfiguration": {
    "AllowCredentials": boolean,
    "AllowHeaders": ["string"],
    "AllowMethods": ["string"],
    "AllowOrigins": ["string"],
    "ExposeHeaders": ["string"],
    "MaxAge": number
  },
  "CreateDate": "string",
  "Description": "string",
  "Name": "string",
  "ProtocolType": "string",
  "RouteSelectionExpression": "string",
  "Version": "string"
},
"AwsApiGatewayV2Stage": {
  "AccessLogSettings": {
    "DestinationArn": "string",
    "Format": "string"
  },
  "ApiGatewayManaged": boolean,
  "AutoDeploy": boolean,
  "ClientCertificateId": "string",
  "CreateDate": "string",
  "DefaultRouteSettings": {
    "DataTraceEnabled": boolean,
    "DetailedMetricsEnabled": boolean,
    "LoggingLevel": "string",
    "ThrottlingBurstLimit": number,
    "ThrottlingRateLimit": number
  },
  "DeploymentId": "string",
  "Description": "string",
  "LastDeploymentStatusMessage": "string",
```

```

    "LastUpdatedDate": "string",
    "RouteSettings": {
      "DetailedMetricsEnabled": boolean,
      "LoggingLevel": "string",
      "DataTraceEnabled": boolean,
      "ThrottlingBurstLimit": number,
      "ThrottlingRateLimit": number
    },
    "StageName": "string",
    "StageVariables": [{
      "string": "string"
    }]
  },
  "AwsAppSyncGraphQLApi": {
    "AwsAppSyncGraphQLApi": {
      "AdditionalAuthenticationProviders": [
        {
          "AuthenticationType": "string",
          "LambdaAuthorizerConfig": {
            "AuthorizerResultTtlInSeconds": integer,
            "AuthorizerUri": "string"
          }
        },
        {
          "AuthenticationType": "string"
        }
      ],
      "ApiId": "string",
      "Arn": "string",
      "AuthenticationType": "string",
      "Id": "string",
      "LogConfig": {
        "CloudWatchLogsRoleArn": "string",
        "ExcludeVerboseContent": boolean,
        "FieldLogLevel": "string"
      },
      "Name": "string",
      "XrayEnabled": boolean
    }
  },
  "AwsAthenaWorkGroup": {
    "Description": "string",
    "Name": "string",
    "WorkgroupConfiguration": {

```

```

    "ResultConfiguration": {
      "EncryptionConfiguration": {
        "EncryptionOption": "string",
        "KmsKey": "string"
      }
    },
    "State": "string"
  },
  "AwsAutoScalingAutoScalingGroup": {
    "AvailabilityZones": [{
      "Value": "string"
    }],
    "CreatedTime": "string",
    "HealthCheckGracePeriod": integer,
    "HealthCheckType": "string",
    "LaunchConfigurationName": "string",
    "LoadBalancerNames": ["string"],
    "LaunchTemplate": {
      "LaunchTemplateId": "string",
      "LaunchTemplateName": "string",
      "Version": "string"
    },
    "MixedInstancesPolicy": {
      "InstancesDistribution": {
        "OnDemandAllocationStrategy": "string",
        "OnDemandBaseCapacity": number,
        "OnDemandPercentageAboveBaseCapacity": number,
        "SpotAllocationStrategy": "string",
        "SpotInstancePools": number,
        "SpotMaxPrice": "string"
      },
      "LaunchTemplate": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "string",
          "LaunchTemplateName": "string",
          "Version": "string"
        },
        "CapacityRebalance": boolean,
        "Overrides": [{
          "InstanceType": "string",
          "WeightedCapacity": "string"
        }]
      }
    }
  }
}

```

```

    }
  },
  "AwsAutoScalingLaunchConfiguration": {
    "AssociatePublicIpAddress": boolean,
    "BlockDeviceMappings": [{
      "DeviceName": "string",
      "Ebs": {
        "DeleteOnTermination": boolean,
        "Encrypted": boolean,
        "Iops": number,
        "SnapshotId": "string",
        "VolumeSize": number,
        "VolumeType": "string"
      },
      "NoDevice": boolean,
      "VirtualName": "string"
    }],
    "ClassicLinkVpcId": "string",
    "ClassicLinkVpcSecurityGroups": ["string"],
    "CreatedTime": "string",
    "EbsOptimized": boolean,
    "IamInstanceProfile": "string"
  },
  "ImageId": "string",
  "InstanceMonitoring": {
    "Enabled": boolean
  },
  "InstanceType": "string",
  "KernelId": "string",
  "KeyName": "string",
  "LaunchConfigurationName": "string",
  "MetadataOptions": {
    "HttpEndPoint": "string",
    "HttpPutReponseHopLimit": number,
    "HttpTokens": "string"
  },
  "PlacementTenancy": "string",
  "RamdiskId": "string",
  "SecurityGroups": ["string"],
  "SpotPrice": "string",
  "UserData": "string"
},
"AwsBackupBackupPlan": {
  "BackupPlan": {

```

```

    "AdvancedBackupSettings": [{
      "BackupOptions": {
        "WindowsVSS": "string"
      },
      "ResourceType": "string"
    }],
    "BackupPlanName": "string",
    "BackupPlanRule": [{
      "CompletionWindowMinutes": integer,
      "CopyActions": [{
        "DestinationBackupVaultArn": "string",
        "Lifecycle": {
          "DeleteAfterDays": integer,
          "MoveToColdStorageAfterDays": integer
        }
      }],
      "Lifecycle": {
        "DeleteAfterDays": integer
      },
      "RuleName": "string",
      "ScheduleExpression": "string",
      "StartWindowMinutes": integer,
      "TargetBackupVault": "string"
    }]
  },
  "BackupPlanArn": "string",
  "BackupPlanId": "string",
  "VersionId": "string"
},
"AwsBackupBackupVault": {
  "AccessPolicy": {
    "Statement": [{
      "Action": ["string"],
      "Effect": "string",
      "Principal": {
        "AWS": "string"
      }
    }],
    "Resource": "string"
  },
  "Version": "string"
},
  "BackupVaultArn": "string",
  "BackupVaultName": "string",
  "EncryptionKeyArn": "string",

```

```

    "Notifications": {
      "BackupVaultEvents": ["string"],
      "SNSTopicArn": "string"
    }
  },
  "AwsBackupRecoveryPoint": {
    "BackupSizeInBytes": integer,
    "BackupVaultName": "string",
    "BackupVaultArn": "string",
    "CalculatedLifecycle": {
      "DeleteAt": "string",
      "MoveToColdStorageAt": "string"
    },
    "CompletionDate": "string",
    "CreatedBy": {
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
      "BackupPlanVersion": "string",
      "BackupRuleId": "string"
    },
    "CreationDate": "string",
    "EncryptionKeyArn": "string",
    "IamRoleArn": "string",
    "IsEncrypted": boolean,
    "LastRestoreTime": "string",
    "Lifecycle": {
      "DeleteAfterDays": integer,
      "MoveToColdStorageAfterDays": integer
    },
    "RecoveryPointArn": "string",
    "ResourceArn": "string",
    "ResourceType": "string",
    "SourceBackupVaultArn": "string",
    "Status": "string",
    "StatusMessage": "string",
    "StorageClass": "string"
  },
  "AwsCertificateManagerCertificate": {
    "CertificateAuthorityArn": "string",
    "CreatedAt": "string",
    "DomainName": "string",
    "DomainValidationOptions": [{
      "DomainName": "string",
      "ResourceRecord": {

```

```
    "Name": "string",
    "Type": "string",
    "Value": "string"
  },
  "ValidationDomain": "string",
  "ValidationEmails": ["string"],
  "ValidationMethod": "string",
  "ValidationStatus": "string"
}],
"ExtendedKeyUsages": [{
  "Name": "string",
  "OId": "string"
}],
"FailureReason": "string",
"ImportedAt": "string",
"InUseBy": ["string"],
"IssuedAt": "string",
"Issuer": "string",
"KeyAlgorithm": "string",
"KeyUsages": [{
  "Name": "string"
}],
"NotAfter": "string",
"NotBefore": "string",
"Options": {
  "CertificateTransparencyLoggingPreference": "string"
},
"RenewalEligibility": "string",
"RenewalSummary": {
  "DomainValidationOptions": [{
    "DomainName": "string",
    "ResourceRecord": {
      "Name": "string",
      "Type": "string",
      "Value": "string"
    },
    "ValidationDomain": "string",
    "ValidationEmails": ["string"],
    "ValidationMethod": "string",
    "ValidationStatus": "string"
  }],
  "RenewalStatus": "string",
  "RenewalStatusReason": "string",
  "UpdatedAt": "string"
```

```

    },
    "Serial": "string",
    "SignatureAlgorithm": "string",
    "Status": "string",
    "Subject": "string",
    "SubjectAlternativeNames": ["string"],
    "Type": "string"
  },
  "AwsCloudFormationStack": {
    "Capabilities": ["string"],
    "CreationTime": "string",
    "Description": "string",
    "DisableRollback": boolean,
    "DriftInformation": {
      "StackDriftStatus": "string"
    },
    "EnableTerminationProtection": boolean,
    "LastUpdatedTime": "string",
    "NotificationArns": ["string"],
    "Outputs": [{
      "Description": "string",
      "OutputKey": "string",
      "OutputValue": "string"
    }],
    "RoleArn": "string",
    "StackId": "string",
    "StackName": "string",
    "StackStatus": "string",
    "StackStatusReason": "string",
    "TimeoutInMinutes": number
  },
  "AwsCloudFrontDistribution": {
    "CacheBehaviors": {
      "Items": [{
        "ViewerProtocolPolicy": "string"
      }]
    },
    "DefaultCacheBehavior": {
      "ViewerProtocolPolicy": "string"
    },
    "DefaultRootObject": "string",
    "DomainName": "string",
    "Etag": "string",
    "LastModifiedTime": "string",

```



```
"Logging": {
  "Bucket": "string",
  "Enabled": boolean,
  "IncludeCookies": boolean,
  "Prefix": "string"
},
"OriginGroups": {
  "Items": [{
    "FailoverCriteria": {
      "StatusCodes": {
        "Items": [number],
        "Quantity": number
      }
    }
  }]
},
"Origins": {
  "Items": [{
    "CustomOriginConfig": {
      "HttpPort": number,
      "HttpsPort": number,
      "OriginKeepaliveTimeout": number,
      "OriginProtocolPolicy": "string",
      "OriginReadTimeout": number,
      "OriginSslProtocols": {
        "Items": ["string"],
        "Quantity": number
      }
    }
  }],
  "DomainName": "string",
  "Id": "string",
  "OriginPath": "string",
  "S3OriginConfig": {
    "OriginAccessIdentity": "string"
  }
},
"Status": "string",
"ViewerCertificate": {
  "AcmCertificateArn": "string",
  "Certificate": "string",
  "CertificateSource": "string",
  "CloudFrontDefaultCertificate": boolean,
  "IamCertificateId": "string",
```

```
    "MinimumProtocolVersion": "string",
    "SslSupportMethod": "string"
  },
  "WebAclId": "string"
},
"AwsCloudTrailTrail": {
  "CloudWatchLogsLogGroupArn": "string",
  "CloudWatchLogsRoleArn": "string",
  "HasCustomEventSelectors": boolean,
  "HomeRegion": "string",
  "IncludeGlobalServiceEvents": boolean,
  "IsMultiRegionTrail": boolean,
  "IsOrganizationTrail": boolean,
  "KmsKeyId": "string",
  "LogFileValidationEnabled": boolean,
  "Name": "string",
  "S3BucketName": "string",
  "S3KeyPrefix": "string",
  "SnsTopicArn": "string",
  "SnsTopicName": "string",
  "TrailArn": "string"
},
"AwsCloudWatchAlarm": {
  "ActionsEnabled": boolean,
  "AlarmActions": ["string"],
  "AlarmArn": "string",
  "AlarmConfigurationUpdatedTimestamp": "string",
  "AlarmDescription": "string",
  "AlarmName": "string",
  "ComparisonOperator": "string",
  "DatapointsToAlarm": number,
  "Dimensions": [{
    "Name": "string",
    "Value": "string"
  }],
  "EvaluateLowSampleCountPercentile": "string",
  "EvaluationPeriods": number,
  "ExtendedStatistic": "string",
  "InsufficientDataActions": ["string"],
  "MetricName": "string",
  "Namespace": "string",
  "OkActions": ["string"],
  "Period": number,
  "Statistic": "string",
```

```

    "Threshold": number,
    "ThresholdMetricId": "string",
    "TreatMissingData": "string",
    "Unit": "string"
  },
  "AwsCodeBuildProject": {
    "Artifacts": [{
      "ArtifactIdentifier": "string",
      "EncryptionDisabled": boolean,
      "Location": "string",
      "Name": "string",
      "NamespaceType": "string",
      "OverrideArtifactName": boolean,
      "Packaging": "string",
      "Path": "string",
      "Type": "string"
    }],
    "SecondaryArtifacts": [{
      "ArtifactIdentifier": "string",
      "Type": "string",
      "Location": "string",
      "Name": "string",
      "NamespaceType": "string",
      "Packaging": "string",
      "Path": "string",
      "EncryptionDisabled": boolean,
      "OverrideArtifactName": boolean
    }],
    "EncryptionKey": "string",
    "Certificate": "string",
    "Environment": {
      "Certificate": "string",
      "EnvironmentVariables": [{
        "Name": "string",
        "Type": "string",
        "Value": "string"
      }],
      "ImagePullCredentialsType": "string",
      "PrivilegedMode": boolean,
      "RegistryCredential": {
        "Credential": "string",
        "CredentialProvider": "string"
      },
      "Type": "string"
    }
  }
}

```

```
},
"LogsConfig": {
  "CloudWatchLogs": {
    "GroupName": "string",
    "Status": "string",
    "StreamName": "string"
  },
  "S3Logs": {
    "EncryptionDisabled": boolean,
    "Location": "string",
    "Status": "string"
  }
},
"Name": "string",
"ServiceRole": "string",
"Source": {
  "Type": "string",
  "Location": "string",
  "GitCloneDepth": integer
},
"VpcConfig": {
  "VpcId": "string",
  "Subnets": ["string"],
  "SecurityGroupIds": ["string"]
},
"AwsDmsEndpoint": {
  "CertificateArn": "string",
  "DatabaseName": "string",
  "EndpointArn": "string",
  "EndpointIdentifier": "string",
  "EndpointType": "string",
  "EngineName": "string",
  "KmsKeyId": "string",
  "Port": integer,
  "ServerName": "string",
  "SslMode": "string",
  "Username": "string"
},
"AwsDmsReplicationInstance": {
  "AllocatedStorage": integer,
  "AutoMinorVersionUpgrade": boolean,
  "AvailabilityZone": "string",
  "EngineVersion": "string",
```

```

    "KmsKeyId": "string",
    "MultiAZ": boolean,
    "PreferredMaintenanceWindow": "string",
    "PubliclyAccessible": boolean,
    "ReplicationInstanceClass": "string",
    "ReplicationInstanceIdentifier": "string",
    "ReplicationSubnetGroup": {
        "ReplicationSubnetGroupIdentifier": "string"
    },
    "VpcSecurityGroups": [
        {
            "VpcSecurityGroupId": "string"
        }
    ],
    "AwsDmsReplicationTask": {
        "CdcStartPosition": "string",
        "Id": "string",
        "MigrationType": "string",
        "ReplicationInstanceArn": "string",
        "ReplicationTaskIdentifier": "string",
        "ReplicationTaskSettings": {
            "string": "string"
        },
        "SourceEndpointArn": "string",
        "TableMappings": {
            "string": "string"
        },
        "TargetEndpointArn": "string"
    },
    "AwsDynamoDbTable": {
        "AttributeDefinitions": [{
            "AttributeName": "string",
            "AttributeType": "string"
        }],
        "BillingModeSummary": {
            "BillingMode": "string",
            "LastUpdateToPayPerRequestDateTime": "string"
        },
        "CreationDateTime": "string",
        "DeletionProtectionEnabled": boolean,
        "GlobalSecondaryIndexes": [{
            "Backfilling": boolean,
            "IndexArn": "string",

```

```
"IndexName": "string",
"IndexSizeBytes": number,
"IndexStatus": "string",
"ItemCount": number,
"KeySchema": [{
  "AttributeName": "string",
  "KeyType": "string"
}],
"Projection": {
  "NonKeyAttributes": ["string"],
  "ProjectionType": "string"
},
"ProvisionedThroughput": {
  "LastDecreaseDateTime": "string",
  "LastIncreaseDateTime": "string",
  "NumberOfDecreasesToday": number,
  "ReadCapacityUnits": number,
  "WriteCapacityUnits": number
}
}],
"GlobalTableVersion": "string",
"ItemCount": number,
"KeySchema": [{
  "AttributeName": "string",
  "KeyType": "string"
}],
"LatestStreamArn": "string",
"LatestStreamLabel": "string",
"LocalSecondaryIndexes": [{
  "IndexArn": "string",
  "IndexName": "string",
  "KeySchema": [{
    "AttributeName": "string",
    "KeyType": "string"
  }
}],
"Projection": {
  "NonKeyAttributes": ["string"],
  "ProjectionType": "string"
}
}],
"ProvisionedThroughput": {
  "LastDecreaseDateTime": "string",
  "LastIncreaseDateTime": "string",
  "NumberOfDecreasesToday": number,
```

```

    "ReadCapacityUnits": number,
    "WriteCapacityUnits": number
  },
  "Replicas": [{
    "GlobalSecondaryIndexes": [{
      "IndexName": "string",
      "ProvisionedThroughputOverride": {
        "ReadCapacityUnits": number
      }
    }],
    "KmsMasterKeyId": "string",
    "ProvisionedThroughputOverride": {
      "ReadCapacityUnits": number
    },
    "RegionName": "string",
    "ReplicaStatus": "string",
    "ReplicaStatusDescription": "string"
  }],
  "RestoreSummary": {
    "RestoreDateTime": "string",
    "RestoreInProgress": boolean,
    "SourceBackupArn": "string",
    "SourceTableArn": "string"
  },
  "SseDescription": {
    "InaccessibleEncryptionDateTime": "string",
    "KmsMasterKeyArn": "string",
    "SseType": "string",
    "Status": "string"
  },
  "StreamSpecification": {
    "StreamEnabled": boolean,
    "StreamViewType": "string"
  },
  "TableId": "string",
  "TableName": "string",
  "TableSizeBytes": number,
  "TableStatus": "string"
},
"AwsEc2ClientVpnEndpoint": {
  "AuthenticationOptions": [
    {
      "MutualAuthentication": {
        "ClientRootCertificateChainArn": "string"
      }
    }
  ]
}

```

```
    },
    "Type": "string"
  }
],
"ClientCidrBlock": "string",
"ClientConnectOptions": {
  "Enabled": boolean
},
"ClientLoginBannerOptions": {
  "Enabled": boolean
},
"ClientVpnEndpointId": "string",
"ConnectionLogOptions": {
  "Enabled": boolean
},
"Description": "string",
"DnsServer": ["string"],
"ServerCertificateArn": "string",
"SecurityGroupIdSet": [
  "string"
],
"SelfServicePortalUrl": "string",
"SessionTimeoutHours": "integer",
"SplitTunnel": boolean,
"TransportProtocol": "string",
"VpcId": "string",
"VpnPort": integer
},
"AwsEc2Eip": {
  "AllocationId": "string",
  "AssociationId": "string",
  "Domain": "string",
  "InstanceId": "string",
  "NetworkBorderGroup": "string",
  "NetworkInterfaceId": "string",
  "NetworkInterfaceOwnerId": "string",
  "PrivateIpAddress": "string",
  "PublicIp": "string",
  "PublicIpv4Pool": "string"
},
"AwsEc2Instance": {
  "IamInstanceProfileArn": "string",
  "ImageId": "string",
  "IPv4Addresses": ["string"],
```



```

    "IPv6Addresses": ["string"],
    "KeyName": "string",
    "LaunchedAt": "string",
    "MetadataOptions": {
      "HttpEndpoint": "string",
      "HttpProtocolIpv6": "string",
      "HttpPutResponseHopLimit": number,
      "HttpTokens": "string",
      "InstanceMetadataTags": "string"
    },
    "Monitoring": {
      "State": "string"
    },
    "NetworkInterfaces": [{
      "NetworkInterfaceId": "string"
    }],
    "SubnetId": "string",
    "Type": "string",
    "VirtualizationType": "string",
    "VpcId": "string"
  },
  "AwsEc2LaunchTemplate": {
    "DefaultVersionNumber": "string",
    "ElasticGpuSpecifications": ["string"],
    "ElasticInferenceAccelerators": ["string"],
    "Id": "string",
    "ImageId": "string",
    "LatestVersionNumber": "string",
    "LaunchTemplateData": {
      "BlockDeviceMappings": [{
        "DeviceName": "string",
        "Ebs": {
          "DeleteonTermination": boolean,
          "Encrypted": boolean,
          "SnapshotId": "string",
          "VolumeSize": number,
          "VolumeType": "string"
        }
      }],
      "MetadataOptions": {
        "HttpTokens": "string",
        "HttpPutResponseHopLimit" : number
      },
      "Monitoring": {

```

```

    "Enabled": boolean
  },
  "NetworkInterfaces": [{
    "AssociatePublicIpAddress" : boolean
  }]
},
"LaunchTemplateName": "string",
"LicenseSpecifications": ["string"],
"SecurityGroupIds": ["string"],
"SecurityGroups": ["string"],
"TagSpecifications": ["string"]
},
"AwsEc2NetworkAcl": {
  "Associations": [{
    "NetworkAclAssociationId": "string",
    "NetworkAclId": "string",
    "SubnetId": "string"
  }],
  "Entries": [{
    "CidrBlock": "string",
    "Egress": boolean,
    "IcmpTypeCode": {
      "Code": number,
      "Type": number
    },
    "Ipv6CidrBlock": "string",
    "PortRange": {
      "From": number,
      "To": number
    },
    "Protocol": "string",
    "RuleAction": "string",
    "RuleNumber": number
  }],
  "IsDefault": boolean,
  "NetworkAclId": "string",
  "OwnerId": "string",
  "VpcId": "string"
},
"AwsEc2NetworkInterface": {
  "Attachment": {
    "AttachmentId": "string",
    "AttachTime": "string",
    "DeleteOnTermination": boolean,

```

```

    "DeviceIndex": number,
    "InstanceId": "string",
    "InstanceOwnerId": "string",
    "Status": "string"
  },
  "Ipv6Addresses": [{
    "Ipv6Address": "string"
  }],
  "NetworkInterfaceId": "string",
  "PrivateIpAddresses": [{
    "PrivateDnsName": "string",
    "PrivateIpAddress": "string"
  }],
  "PublicDnsName": "string",
  "PublicIp": "string",
  "SecurityGroups": [{
    "GroupId": "string",
    "GroupName": "string"
  }],
  "SourceDestCheck": boolean
},
"AwsEc2RouteTable": {
  "AssociationSet": [{
    "AssociationState": {
      "State": "string"
    },
    "Main": boolean,
    "RouteTableAssociationId": "string",
    "RouteTableId": "string"
  }],
  "PropagatingVgwSet": [],
  "RouteTableId": "string",
  "RouteSet": [
    {
      "DestinationCidrBlock": "string",
      "GatewayId": "string",
      "Origin": "string",
      "State": "string"
    },
    {
      "DestinationCidrBlock": "string",
      "GatewayId": "string",
      "Origin": "string",
      "State": "string"
    }
  ]
}

```

```

    }
  ],
  "VpcId": "string"
},
"AwsEc2SecurityGroup": {
  "GroupId": "string",
  "GroupName": "string",
  "IpPermissions": [{
    "FromPort": number,
    "IpProtocol": "string",
    "IpRanges": [{
      "CidrIp": "string"
    }],
    "Ipv6Ranges": [{
      "CidrIpv6": "string"
    }],
    "PrefixListIds": [{
      "PrefixListId": "string"
    }],
    "ToPort": number,
    "UserIdGroupPairs": [{
      "GroupId": "string",
      "GroupName": "string",
      "PeeringStatus": "string",
      "UserId": "string",
      "VpcId": "string",
      "VpcPeeringConnectionId": "string"
    }]
  }],
  "IpPermissionsEgress": [{
    "FromPort": number,
    "IpProtocol": "string",
    "IpRanges": [{
      "CidrIp": "string"
    }],
    "Ipv6Ranges": [{
      "CidrIpv6": "string"
    }],
    "PrefixListIds": [{
      "PrefixListId": "string"
    }],
    "ToPort": number,
    "UserIdGroupPairs": [{
      "GroupId": "string",

```

```

    "GroupName": "string",
    "PeeringStatus": "string",
    "UserId": "string",
    "VpcId": "string",
    "VpcPeeringConnectionId": "string"
  ]
}],
  "OwnerId": "string",
  "VpcId": "string"
},
  "AwsEc2Subnet": {
    "AssignIpv6AddressOnCreation": boolean,
    "AvailabilityZone": "string",
    "AvailabilityZoneId": "string",
    "AvailableIpAddressCount": number,
    "CidrBlock": "string",
    "DefaultForAz": boolean,
    "Ipv6CidrBlockAssociationSet": [{
      "AssociationId": "string",
      "Ipv6CidrBlock": "string",
      "CidrBlockState": "string"
    }],
    "MapPublicIpOnLaunch": boolean,
    "OwnerId": "string",
    "State": "string",
    "SubnetArn": "string",
    "SubnetId": "string",
    "VpcId": "string"
  },
  "AwsEc2TransitGateway": {
    "AmazonSideAsn": number,
    "AssociationDefaultRouteTableId": "string",
    "AutoAcceptSharedAttachments": "string",
    "DefaultRouteTableAssociation": "string",
    "DefaultRouteTablePropagation": "string",
    "Description": "string",
    "DnsSupport": "string",
    "Id": "string",
    "MulticastSupport": "string",
    "PropagationDefaultRouteTableId": "string",
    "TransitGatewayCidrBlocks": ["string"],
    "VpnEcmpSupport": "string"
  },
  "AwsEc2Volume": {

```

```

"Attachments": [{
  "AttachTime": "string",
  "DeleteOnTermination": boolean,
  "InstanceId": "string",
  "Status": "string"
}],
"CreateTime": "string",
"DeviceName": "string",
"Encrypted": boolean,
"KmsKeyId": "string",
"Size": number,
"SnapshotId": "string",
"Status": "string",
"VolumeId": "string",
"VolumeScanStatus": "string",
"VolumeType": "string"
},
"AwsEc2Vpc": {
  "CidrBlockAssociationSet": [{
    "AssociationId": "string",
    "CidrBlock": "string",
    "CidrBlockState": "string"
  }],
  "DhcpOptionsId": "string",
  "Ipv6CidrBlockAssociationSet": [{
    "AssociationId": "string",
    "CidrBlockState": "string",
    "Ipv6CidrBlock": "string"
  }],
  "State": "string"
},
"AwsEc2VpcEndpointService": {
  "AcceptanceRequired": boolean,
  "AvailabilityZones": ["string"],
  "BaseEndpointDnsNames": ["string"],
  "ManagesVpcEndpoints": boolean,
  "GatewayLoadBalancerArns": ["string"],
  "NetworkLoadBalancerArns": ["string"],
  "PrivateDnsName": "string",
  "ServiceId": "string",
  "ServiceName": "string",
  "ServiceState": "string",
  "ServiceType": [{
    "ServiceType": "string"
  }],

```

```

    ]]
  },
  "AwsEc2VpcPeeringConnection": {
    "AcceptorVpcInfo": {
      "CidrBlock": "string",
      "CidrBlockSet": [{
        "CidrBlock": "string"
      }],
      "Ipv6CidrBlockSet": [{
        "Ipv6CidrBlock": "string"
      }],
      "OwnerId": "string",
      "PeeringOptions": {
        "AllowDnsResolutionFromRemoteVpc": boolean,
        "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
        "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
      },
      "Region": "string",
      "VpcId": "string"
    },
    "ExpirationTime": "string",
    "RequesterVpcInfo": {
      "CidrBlock": "string",
      "CidrBlockSet": [{
        "CidrBlock": "string"
      }],
      "Ipv6CidrBlockSet": [{
        "Ipv6CidrBlock": "string"
      }],
      "OwnerId": "string",
      "PeeringOptions": {
        "AllowDnsResolutionFromRemoteVpc": boolean,
        "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
        "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
      },
      "Region": "string",
      "VpcId": "string"
    },
    "Status": {
      "Code": "string",
      "Message": "string"
    },
    "VpcPeeringConnectionId": "string"
  },

```

```
"AwsEcrContainerImage": {
  "Architecture": "string",
  "ImageDigest": "string",
  "ImagePublishedAt": "string",
  "ImageTags": ["string"],
  "RegistryId": "string",
  "RepositoryName": "string"
},
"AwsEcrRepository": {
  "Arn": "string",
  "ImageScanningConfiguration": {
    "ScanOnPush": boolean
  },
  "ImageTagMutability": "string",
  "LifecyclePolicy": {
    "LifecyclePolicyText": "string",
    "RegistryId": "string"
  },
  "RepositoryName": "string",
  "RepositoryPolicyText": "string"
},
"AwsEcsCluster": {
  "ActiveServicesCount": number,
  "CapacityProviders": ["string"],
  "ClusterArn": "string",
  "ClusterName": "string",
  "ClusterSettings": [{
    "Name": "string",
    "Value": "string"
  }],
  "Configuration": {
    "ExecuteCommandConfiguration": {
      "KmsKeyId": "string",
      "LogConfiguration": {
        "CloudWatchEncryptionEnabled": boolean,
        "CloudWatchLogGroupName": "string",
        "S3BucketName": "string",
        "S3EncryptionEnabled": boolean,
        "S3KeyPrefix": "string"
      },
      "Logging": "string"
    }
  },
  "DefaultCapacityProviderStrategy": [{
```



```

    "Base": number,
    "CapacityProvider": "string",
    "Weight": number
  ]],
  "RegisteredContainerInstancesCount": number,
  "RunningTasksCount": number,
  "Status": "string"
},
"AwsEcsContainer": {
  "Image": "string",
  "MountPoints": [{
    "ContainerPath": "string",
    "SourceVolume": "string"
  }],
  "Name": "string",
  "Privileged": boolean
},
"AwsEcsService": {
  "CapacityProviderStrategy": [{
    "Base": number,
    "CapacityProvider": "string",
    "Weight": number
  }],
  "Cluster": "string",
  "DeploymentConfiguration": {
    "DeploymentCircuitBreaker": {
      "Enable": boolean,
      "Rollback": boolean
    },
    "MaximumPercent": number,
    "MinimumHealthyPercent": number
  },
  "DeploymentController": {
    "Type": "string"
  },
  "DesiredCount": number,
  "EnableEcsManagedTags": boolean,
  "EnableExecuteCommand": boolean,
  "HealthCheckGracePeriodSeconds": number,
  "LaunchType": "string",
  "LoadBalancers": [{
    "ContainerName": "string",
    "ContainerPort": number,
    "LoadBalancerName": "string",

```

```

    "TargetGroupArn": "string"
  }],
  "Name": "string",
  "NetworkConfiguration": {
    "AwsVpcConfiguration": {
      "AssignPublicIp": "string",
      "SecurityGroups": ["string"],
      "Subnets": ["string"]
    }
  },
  "PlacementConstraints": [{
    "Expression": "string",
    "Type": "string"
  }],
  "PlacementStrategies": [{
    "Field": "string",
    "Type": "string"
  }],
  "PlatformVersion": "string",
  "PropagateTags": "string",
  "Role": "string",
  "SchedulingStrategy": "string",
  "ServiceArn": "string",
  "ServiceName": "string",
  "ServiceRegistries": [{
    "ContainerName": "string",
    "ContainerPort": number,
    "Port": number,
    "RegistryArn": "string"
  }],
  "TaskDefinition": "string"
},
"AwsEcsTask": {
  "CreatedAt": "string",
  "ClusterArn": "string",
  "Group": "string",
  "StartedAt": "string",
  "StartedBy": "string",
  "TaskDefinitionArn": "string",
  "Version": number,
  "Volumes": [{
    "Name": "string",
    "Host": {
      "SourcePath": "string"
    }
  }
}

```

```

    }
  ]],
  "Containers": [{
    "Image": "string",
    "MountPoints": [{
      "ContainerPath": "string",
      "SourceVolume": "string"
    }],
    "Name": "string",
    "Privileged": boolean
  }]
},
"AwsEcsTaskDefinition": {
  "ContainerDefinitions": [{
    "Command": ["string"],
    "Cpu": number,
    "DependsOn": [{
      "Condition": "string",
      "ContainerName": "string"
    }],
    "DisableNetworking": boolean,
    "DnsSearchDomains": ["string"],
    "DnsServers": ["string"],
    "DockerLabels": {
      "string": "string"
    },
    "DockerSecurityOptions": ["string"],
    "EntryPoint": ["string"],
    "Environment": [{
      "Name": "string",
      "Value": "string"
    }],
    "EnvironmentFiles": [{
      "Type": "string",
      "Value": "string"
    }],
    "Essential": boolean,
    "ExtraHosts": [{
      "Hostname": "string",
      "IpAddress": "string"
    }],
    "FirelensConfiguration": {
      "Options": {
        "string": "string"
      }
    }
  ]
}

```

```
    },
    "Type": "string"
  },
  "HealthCheck": {
    "Command": ["string"],
    "Interval": number,
    "Retries": number,
    "StartPeriod": number,
    "Timeout": number
  },
  "Hostname": "string",
  "Image": "string",
  "Interactive": boolean,
  "Links": ["string"],
  "LinuxParameters": {
    "Capabilities": {
      "Add": ["string"],
      "Drop": ["string"]
    },
    "Devices": [{
      "ContainerPath": "string",
      "HostPath": "string",
      "Permissions": ["string"]
    }],
    "InitProcessEnabled": boolean,
    "MaxSwap": number,
    "SharedMemorySize": number,
    "Swappiness": number,
    "Tmpfs": [{
      "ContainerPath": "string",
      "MountOptions": ["string"],
      "Size": number
    }]
  },
  "LogConfiguration": {
    "LogDriver": "string",
    "Options": {
      "string": "string"
    },
    "SecretOptions": [{
      "Name": "string",
      "ValueFrom": "string"
    }]
  }
},
```

```
"Memory": number,
"MemoryReservation": number,
"MountPoints": [{
  "ContainerPath": "string",
  "ReadOnly": boolean,
  "SourceVolume": "string"
}],
"Name": "string",
"PortMappings": [{
  "ContainerPort": number,
  "HostPort": number,
  "Protocol": "string"
}],
"Privileged": boolean,
"PseudoTerminal": boolean,
"ReadonlyRootFilesystem": boolean,
"RepositoryCredentials": {
  "CredentialsParameter": "string"
},
"ResourceRequirements": [{
  "Type": "string",
  "Value": "string"
}],
"Secrets": [{
  "Name": "string",
  "ValueFrom": "string"
}],
"StartTimeout": number,
"StopTimeout": number,
"SystemControls": [{
  "Namespace": "string",
  "Value": "string"
}],
"Ulimits": [{
  "HardLimit": number,
  "Name": "string",
  "SoftLimit": number
}],
"User": "string",
"VolumesFrom": [{
  "ReadOnly": boolean,
  "SourceContainer": "string"
}],
"WorkingDirectory": "string"
```

```

    }],
    "Cpu": "string",
    "ExecutionRoleArn": "string",
    "Family": "string",
    "InferenceAccelerators": [{
      "DeviceName": "string",
      "DeviceType": "string"
    }],
    "IpcMode": "string",
    "Memory": "string",
    "NetworkMode": "string",
    "PidMode": "string",
    "PlacementConstraints": [{
      "Expression": "string",
      "Type": "string"
    }],
    "ProxyConfiguration": {
      "ContainerName": "string",
      "ProxyConfigurationProperties": [{
        "Name": "string",
        "Value": "string"
      }],
      "Type": "string"
    },
    "RequiresCompatibilities": ["string"],
    "Status": "string",
    "TaskRoleArn": "string",
    "Volumes": [{
      "DockerVolumeConfiguration": {
        "Autoprovision": boolean,
        "Driver": "string",
        "DriverOpts": {
          "string": "string"
        },
        "Labels": {
          "string": "string"
        },
        "Scope": "string"
      },
      "EfsVolumeConfiguration": {
        "AuthorizationConfig": {
          "AccessPointId": "string",
          "Iam": "string"
        },

```

```

    "FilesystemId": "string",
    "RootDirectory": "string",
    "TransitEncryption": "string",
    "TransitEncryptionPort": number
  },
  "Host": {
    "SourcePath": "string"
  },
  "Name": "string"
}]
},
"AwsEfsAccessPoint": {
  "AccessPointId": "string",
  "Arn": "string",
  "ClientToken": "string",
  "FileSystemId": "string",
  "PosixUser": {
    "Gid": "string",
    "SecondaryGids": ["string"],
    "Uid": "string"
  },
  "RootDirectory": {
    "CreationInfo": {
      "OwnerGid": "string",
      "OwnerUid": "string",
      "Permissions": "string"
    },
    "Path": "string"
  }
},
"AwsEksCluster": {
  "Arn": "string",
  "CertificateAuthorityData": "string",
  "ClusterStatus": "string",
  "Endpoint": "string",
  "Logging": {
    "ClusterLogging": [{
      "Enabled": boolean,
      "Types": ["string"]
    }]
  },
  "Name": "string",
  "ResourcesVpcConfig": {
    "EndpointPublicAccess": boolean,

```

```

    "SecurityGroupIds": ["string"],
    "SubnetIds": ["string"]
  },
  "RoleArn": "string",
  "Version": "string"
},
"AwsElasticBeanstalkEnvironment": {
  "ApplicationName": "string",
  "Cname": "string",
  "DateCreated": "string",
  "DateUpdated": "string",
  "Description": "string",
  "EndpointUrl": "string",
  "EnvironmentArn": "string",
  "EnvironmentId": "string",
  "EnvironmentLinks": [{
    "EnvironmentName": "string",
    "LinkName": "string"
  }],
  "EnvironmentName": "string",
  "OptionSettings": [{
    "Namespace": "string",
    "OptionName": "string",
    "ResourceName": "string",
    "Value": "string"
  }],
  "PlatformArn": "string",
  "SolutionStackName": "string",
  "Status": "string",
  "Tier": {
    "Name": "string",
    "Type": "string",
    "Version": "string"
  },
  "VersionLabel": "string"
},
"AwsElasticSearchDomain": {
  "AccessPolicies": "string",
  "DomainStatus": {
    "DomainId": "string",
    "DomainName": "string",
    "Endpoint": "string",
    "Endpoints": {
      "string": "string"
    }
  }
}

```



```
    }
  },
  "DomainEndpointOptions": {
    "EnforceHTTPS": boolean,
    "TLSSecurityPolicy": "string"
  },
  "ElasticsearchClusterConfig": {
    "DedicatedMasterCount": number,
    "DedicatedMasterEnabled": boolean,
    "DedicatedMasterType": "string",
    "InstanceCount": number,
    "InstanceType": "string",
    "ZoneAwarenessConfig": {
      "AvailabilityZoneCount": number
    },
    "ZoneAwarenessEnabled": boolean
  },
  "ElasticsearchVersion": "string",
  "EncryptionAtRestOptions": {
    "Enabled": boolean,
    "KmsKeyId": "string"
  },
  "LogPublishingOptions": {
    "AuditLogs": {
      "CloudWatchLogsLogGroupArn": "string",
      "Enabled": boolean
    },
    "IndexSlowLogs": {
      "CloudWatchLogsLogGroupArn": "string",
      "Enabled": boolean
    },
    "SearchSlowLogs": {
      "CloudWatchLogsLogGroupArn": "string",
      "Enabled": boolean
    }
  },
  "NodeToNodeEncryptionOptions": {
    "Enabled": boolean
  },
  "ServiceSoftwareOptions": {
    "AutomatedUpdateDate": "string",
    "Cancellable": boolean,
    "CurrentVersion": "string",
    "Description": "string",
```

```
    "NewVersion": "string",
    "UpdateAvailable": boolean,
    "UpdateStatus": "string"
  },
  "VPCOptions": {
    "AvailabilityZones": [
      "string"
    ],
    "SecurityGroupIds": [
      "string"
    ],
    "SubnetIds": [
      "string"
    ],
    "VPCId": "string"
  }
},
"AwsElbLoadBalancer": {
  "AvailabilityZones": ["string"],
  "BackendServerDescriptions": [{
    "InstancePort": number,
    "PolicyNames": ["string"]
  }],
  "CanonicalHostedZoneName": "string",
  "CanonicalHostedZoneNameID": "string",
  "CreatedTime": "string",
  "DnsName": "string",
  "HealthCheck": {
    "HealthyThreshold": number,
    "Interval": number,
    "Target": "string",
    "Timeout": number,
    "UnhealthyThreshold": number
  },
  "Instances": [{
    "InstanceId": "string"
  }],
  "ListenerDescriptions": [{
    "Listener": {
      "InstancePort": number,
      "InstanceProtocol": "string",
      "LoadBalancerPort": number,
      "Protocol": "string",
      "SslCertificateId": "string"
    }
  ]
}
```

```

    },
    "PolicyNames": ["string"]
  ]],
  "LoadBalancerAttributes": {
    "AccessLog": {
      "EmitInterval": number,
      "Enabled": boolean,
      "S3BucketName": "string",
      "S3BucketPrefix": "string"
    },
    "ConnectionDraining": {
      "Enabled": boolean,
      "Timeout": number
    },
    "ConnectionSettings": {
      "IdleTimeout": number
    },
    "CrossZoneLoadBalancing": {
      "Enabled": boolean
    },
    "AdditionalAttributes": [{
      "Key": "string",
      "Value": "string"
    }]
  },
  "LoadBalancerName": "string",
  "Policies": {
    "AppCookieStickinessPolicies": [{
      "CookieName": "string",
      "PolicyName": "string"
    }],
    "LbCookieStickinessPolicies": [{
      "CookieExpirationPeriod": number,
      "PolicyName": "string"
    }],
    "OtherPolicies": ["string"]
  },
  "Scheme": "string",
  "SecurityGroups": ["string"],
  "SourceSecurityGroup": {
    "GroupName": "string",
    "OwnerAlias": "string"
  },
  "Subnets": ["string"],

```

```

    "VpcId": "string"
  },
  "AwsElbv2LoadBalancer": {
    "AvailabilityZones": {
      "SubnetId": "string",
      "ZoneName": "string"
    },
    "CanonicalHostedZoneId": "string",
    "CreateTime": "string",
    "DNSName": "string",
    "IpAddressType": "string",
    "LoadBalancerAttributes": [{
      "Key": "string",
      "Value": "string"
    }],
    "Scheme": "string",
    "SecurityGroups": ["string"],
    "State": {
      "Code": "string",
      "Reason": "string"
    },
    "Type": "string",
    "VpcId": "string"
  },
  "AwsEventSchemasRegistry": {
    "Description": "string",
    "RegistryArn": "string",
    "RegistryName": "string"
  },
  "AwsEventsEndpoint": {
    "Arn": "string",
    "Description": "string",
    "EndpointId": "string",
    "EndpointUrl": "string",
    "EventBuses": [
      {
        "EventBusArn": "string"
      },
      {
        "EventBusArn": "string"
      }
    ],
    "Name": "string",
    "ReplicationConfig": {

```

```

    "State": "string"
  },
  "RoleArn": "string",
  "RoutingConfig": {
    "FailoverConfig": {
      "Primary": {
        "HealthCheck": "string"
      },
      "Secondary": {
        "Route": "string"
      }
    }
  },
  "State": "string"
},
"EventsEventBus": {
  "Arn": "string",
  "Name": "string",
  "Policy": "string"
},
"GuardDutyDetector": {
  "FindingPublishingFrequency": "string",
  "ServiceRole": "string",
  "Status": "string",
  "DataSources": {
    "CloudTrail": {
      "Status": "string"
    },
    "DnsLogs": {
      "Status": "string"
    },
    "FlowLogs": {
      "Status": "string"
    },
    "S3Logs": {
      "Status": "string"
    },
    "Kubernetes": {
      "AuditLogs": {
        "Status": "string"
      }
    }
  },
  "MalwareProtection": {
    "ScanEc2InstanceWithFindings": {

```

```

    "EbsVolumes": {
      "Status": "string"
    }
  },
  "ServiceRole": "string"
}
},
"AwsIamAccessKey": {
  "AccessKeyId": "string",
  "AccountId": "string",
  "CreatedAt": "string",
  "PrincipalId": "string",
  "PrincipalName": "string",
  "PrincipalType": "string",
  "SessionContext": {
    "Attributes": {
      "CreationDate": "string",
      "MfaAuthenticated": boolean
    },
    "SessionIssuer": {
      "AccountId": "string",
      "Arn": "string",
      "PrincipalId": "string",
      "Type": "string",
      "UserName": "string"
    }
  },
  "Status": "string"
},
"AwsIamGroup": {
  "AttachedManagedPolicies": [{
    "PolicyArn": "string",
    "PolicyName": "string"
  }],
  "CreateDate": "string",
  "GroupId": "string",
  "GroupName": "string",
  "GroupPolicyList": [{
    "PolicyName": "string"
  }],
  "Path": "string"
},
"AwsIamPolicy": {

```

```

    "AttachmentCount": number,
    "CreateDate": "string",
    "DefaultVersionId": "string",
    "Description": "string",
    "IsAttachable": boolean,
    "Path": "string",
    "PermissionsBoundaryUsageCount": number,
    "PolicyId": "string",
    "PolicyName": "string",
    "PolicyVersionList": [{
      "CreateDate": "string",
      "IsDefaultVersion": boolean,
      "VersionId": "string"
    }],
    "UpdateDate": "string"
  },
  "AwsIamRole": {
    "AssumeRolePolicyDocument": "string",
    "AttachedManagedPolicies": [{
      "PolicyArn": "string",
      "PolicyName": "string"
    }],
    "CreateDate": "string",
    "InstanceProfileList": [{
      "Arn": "string",
      "CreateDate": "string",
      "InstanceProfileId": "string",
      "InstanceProfileName": "string",
      "Path": "string",
      "Roles": [{
        "Arn": "string",
        "AssumeRolePolicyDocument": "string",
        "CreateDate": "string",
        "Path": "string",
        "RoleId": "string",
        "RoleName": "string"
      }]
    }],
    "MaxSessionDuration": number,
    "Path": "string",
    "PermissionsBoundary": {
      "PermissionsBoundaryArn": "string",
      "PermissionsBoundaryType": "string"
    }
  },

```

```
"RoleId": "string",
"RoleName": "string",
"RolePolicyList": [{
  "PolicyName": "string"
}]
},
"AwsIamUser": {
  "AttachedManagedPolicies": [{
    "PolicyArn": "string",
    "PolicyName": "string"
  }],
  "CreateDate": "string",
  "GroupList": ["string"],
  "Path": "string",
  "PermissionsBoundary": {
    "PermissionsBoundaryArn": "string",
    "PermissionsBoundaryType": "string"
  },
  "UserId": "string",
  "UserName": "string",
  "UserPolicyList": [{
    "PolicyName": "string"
  }]
},
"AwsKinesisStream": {
  "Arn": "string",
  "Name": "string",
  "RetentionPeriodHours": number,
  "ShardCount": number,
  "StreamEncryption": {
    "EncryptionType": "string",
    "KeyId": "string"
  }
},
"AwsKmsKey": {
  "AWSAccountId": "string",
  "CreationDate": "string",
  "Description": "string",
  "KeyId": "string",
  "KeyManager": "string",
  "KeyRotationStatus": boolean,
  "KeyState": "string",
  "Origin": "string"
},
```



```
"AwsLambdaFunction": {
  "Architectures": [
    "string"
  ],
  "Code": {
    "S3Bucket": "string",
    "S3Key": "string",
    "S3ObjectVersion": "string",
    "ZipFile": "string"
  },
  "CodeSha256": "string",
  "DeadLetterConfig": {
    "TargetArn": "string"
  },
  "Environment": {
    "Variables": {
      "Stage": "string"
    }
  },
  "Error": {
    "ErrorCode": "string",
    "Message": "string"
  }
},
"FunctionName": "string",
"Handler": "string",
"KmsKeyArn": "string",
"LastModified": "string",
"Layers": {
  "Arn": "string",
  "CodeSize": number
},
"PackageType": "string",
"RevisionId": "string",
"Role": "string",
"Runtime": "string",
"Timeout": integer,
"TracingConfig": {
  "Mode": "string"
},
"Version": "string",
"VpcConfig": {
  "SecurityGroupIds": ["string"],
  "SubnetIds": ["string"]
},

```

```
    "MasterArn": "string",
    "MemorySize": number
  },
  "AwsLambdaLayerVersion": {
    "CompatibleRuntimes": [
      "string"
    ],
    "CreateDate": "string",
    "Version": number
  },
  "AwsMskCluster": {
    "ClusterInfo": {
      "ClientAuthentication": {
        "Sasl": {
          "Scram": {
            "Enabled": boolean
          },
          "Iam": {
            "Enabled": boolean
          }
        },
        "Tls": {
          "CertificateAuthorityArnList": [],
          "Enabled": boolean
        },
        "Unauthenticated": {
          "Enabled": boolean
        }
      },
      "ClusterName": "string",
      "CurrentVersion": "string",
      "EncryptionInfo": {
        "EncryptionAtRest": {
          "DataVolumeKMSKeyId": "string"
        },
        "EncryptionInTransit": {
          "ClientBroker": "string",
          "InCluster": boolean
        }
      },
      "EnhancedMonitoring": "string",
      "NumberOfBrokerNodes": integer
    }
  },
}
```

```

"AwsNetworkFirewallFirewall": {
  "DeleteProtection": boolean,
  "Description": "string",
  "FirewallArn": "string",
  "FirewallId": "string",
  "FirewallName": "string",
  "FirewallPolicyArn": "string",
  "FirewallPolicyChangeProtection": boolean,
  "SubnetChangeProtection": boolean,
  "SubnetMappings": [{
    "SubnetId": "string"
  }],
  "VpcId": "string"
},
"AwsNetworkFirewallFirewallPolicy": {
  "Description": "string",
  "FirewallPolicy": {
    "StatefulRuleGroupReferences": [{
      "ResourceArn": "string"
    }],
    "StatelessCustomActions": [{
      "ActionDefinition": {
        "PublishMetricAction": {
          "Dimensions": [{
            "Value": "string"
          }]
        }
      }
    ]
  },
  "ActionName": "string"
}],
  "StatelessDefaultActions": ["string"],
  "StatelessFragmentDefaultActions": ["string"],
  "StatelessRuleGroupReferences": [{
    "Priority": number,
    "ResourceArn": "string"
  }]
},
  "FirewallPolicyArn": "string",
  "FirewallPolicyId": "string",
  "FirewallPolicyName": "string"
},
"AwsNetworkFirewallRuleGroup": {
  "Capacity": number,
  "Description": "string",

```

```
"RuleGroup": {
  "RulesSource": {
    "RulesSourceList": {
      "GeneratedRulesType": "string",
      "Targets": ["string"],
      "TargetTypes": ["string"]
    },
    "RulesString": "string",
    "StatefulRules": [{
      "Action": "string",
      "Header": {
        "Destination": "string",
        "DestinationPort": "string",
        "Direction": "string",
        "Protocol": "string",
        "Source": "string",
        "SourcePort": "string"
      },
      "RuleOptions": [{
        "Keyword": "string",
        "Settings": ["string"]
      }]
    }],
    "StatelessRulesAndCustomActions": {
      "CustomActions": [{
        "ActionDefinition": {
          "PublishMetricAction": {
            "Dimensions": [{
              "Value": "string"
            }]
          }
        },
        "ActionName": "string"
      }],
      "StatelessRules": [{
        "Priority": number,
        "RuleDefinition": {
          "Actions": ["string"],
          "MatchAttributes": {
            "DestinationPorts": [{
              "FromPort": number,
              "ToPort": number
            }],
            "Destinations": [{
```

```

        "AddressDefinition": "string"
    ]],
    "Protocols": [number],
    "SourcePorts": [{
        "FromPort": number,
        "ToPort": number
    }],
    "Sources": [{
        "AddressDefinition": "string"
    }],
    "TcpFlags": [{
        "Flags": ["string"],
        "Masks": ["string"]
    }]
}
}
]]
}
},
"RuleVariables": {
    "IpSets": {
        "Definition": ["string"]
    },
    "PortSets": {
        "Definition": ["string"]
    }
}
},
"RuleGroupArn": "string",
"RuleGroupId": "string",
"RuleGroupName": "string",
"Type": "string"
},
"awsOpenSearchServiceDomain": {
    "AccessPolicies": "string",
    "AdvancedSecurityOptions": {
        "Enabled": boolean,
        "InternalUserDatabaseEnabled": boolean,
        "MasterUserOptions": {
            "MasterUserArn": "string",
            "MasterUserName": "string",
            "MasterUserPassword": "string"
        }
    }
},

```

```
"Arn": "string",
"ClusterConfig": {
  "DedicatedMasterCount": number,
  "DedicatedMasterEnabled": boolean,
  "DedicatedMasterType": "string",
  "InstanceCount": number,
  "InstanceType": "string",
  "WarmCount": number,
  "WarmEnabled": boolean,
  "WarmType": "string",
  "ZoneAwarenessConfig": {
    "AvailabilityZoneCount": number
  },
  "ZoneAwarenessEnabled": boolean
},
"DomainEndpoint": "string",
"DomainEndpointOptions": {
  "CustomEndpoint": "string",
  "CustomEndpointCertificateArn": "string",
  "CustomEndpointEnabled": boolean,
  "EnforceHTTPS": boolean,
  "TLSSecurityPolicy": "string"
},
"DomainEndpoints": {
  "string": "string"
},
"DomainName": "string",
"EncryptionAtRestOptions": {
  "Enabled": boolean,
  "KmsKeyId": "string"
},
"EngineVersion": "string",
"Id": "string",
"LogPublishingOptions": {
  "AuditLogs": {
    "CloudWatchLogsLogGroupArn": "string",
    "Enabled": boolean
  },
  "IndexSlowLogs": {
    "CloudWatchLogsLogGroupArn": "string",
    "Enabled": boolean
  },
  "SearchSlowLogs": {
    "CloudWatchLogsLogGroupArn": "string",
```

```

    "Enabled": boolean
  },
  "NodeToNodeEncryptionOptions": {
    "Enabled": boolean
  },
  "ServiceSoftwareOptions": {
    "AutomatedUpdateDate": "string",
    "Cancellable": boolean,
    "CurrentVersion": "string",
    "Description": "string",
    "NewVersion": "string",
    "OptionalDeployment": boolean,
    "UpdateAvailable": boolean,
    "UpdateStatus": "string"
  },
  "VpcOptions": {
    "SecurityGroupIds": ["string"],
    "SubnetIds": ["string"]
  },
},
"AwsRdsDbCluster": {
  "ActivityStreamStatus": "string",
  "AllocatedStorage": number,
  "AssociatedRoles": [{
    "RoleArn": "string",
    "Status": "string"
  }],
  "AutoMinorVersionUpgrade": boolean,
  "AvailabilityZones": ["string"],
  "BackupRetentionPeriod": integer,
  "ClusterCreateTime": "string",
  "CopyTagsToSnapshot": boolean,
  "CrossAccountClone": boolean,
  "CustomEndpoints": ["string"],
  "DatabaseName": "string",
  "DbClusterIdentifier": "string",
  "DbClusterMembers": [{
    "DbClusterParameterGroupStatus": "string",
    "DbInstanceIdentifier": "string",
    "IsClusterWriter": boolean,
    "PromotionTier": integer
  }],
  "DbClusterOptionGroupMemberships": [{

```

```

    "DbClusterOptionGroupName": "string",
    "Status": "string"
  }],
  "DbClusterParameterGroup": "string",
  "DbClusterResourceId": "string",
  "DbSubnetGroup": "string",
  "DeletionProtection": boolean,
  "DomainMemberships": [{
    "Domain": "string",
    "Fqdn": "string",
    "IamRoleName": "string",
    "Status": "string"
  }],
  "EnabledCloudwatchLogsExports": ["string"],
  "Endpoint": "string",
  "Engine": "string",
  "EngineMode": "string",
  "EngineVersion": "string",
  "HostedZoneId": "string",
  "HttpEndpointEnabled": boolean,
  "IamDatabaseAuthenticationEnabled": boolean,
  "KmsKeyId": "string",
  "MasterUsername": "string",
  "MultiAz": boolean,
  "Port": integer,
  "PreferredBackupWindow": "string",
  "PreferredMaintenanceWindow": "string",
  "ReaderEndpoint": "string",
  "ReadReplicaIdentifiers": ["string"],
  "Status": "string",
  "StorageEncrypted": boolean,
  "VpcSecurityGroups": [{
    "Status": "string",
    "VpcSecurityGroupId": "string"
  }]
},
"awsRdsDbClusterSnapshot": {
  "AllocatedStorage": integer,
  "AvailabilityZones": ["string"],
  "ClusterCreateTime": "string",
  "DbClusterIdentifier": "string",
  "DbClusterSnapshotAttributes": [{
    "AttributeName": "string",
    "AttributeValues": ["string"]
  }]
}

```



```

    }],
    "DbClusterSnapshotIdentifier": "string",
    "Engine": "string",
    "EngineVersion": "string",
    "IamDatabaseAuthenticationEnabled": boolean,
    "KmsKeyId": "string",
    "LicenseModel": "string",
    "MasterUsername": "string",
    "PercentProgress": integer,
    "Port": integer,
    "SnapshotCreateTime": "string",
    "SnapshotType": "string",
    "Status": "string",
    "StorageEncrypted": boolean,
    "VpcId": "string"
  },
  "AwsRdsDbInstance": {
    "AllocatedStorage": number,
    "AssociatedRoles": [{
      "RoleArn": "string",
      "FeatureName": "string",
      "Status": "string"
    }],
    "AutoMinorVersionUpgrade": boolean,
    "AvailabilityZone": "string",
    "BackupRetentionPeriod": number,
    "CACertificateIdentifier": "string",
    "CharacterSetName": "string",
    "CopyTagsToSnapshot": boolean,
    "DBClusterIdentifier": "string",
    "DBInstanceClass": "string",
    "DBInstanceIdentifier": "string",
    "DbInstancePort": number,
    "DbInstanceStatus": "string",
    "DbiResourceId": "string",
    "DBName": "string",
    "DbParameterGroups": [{
      "DbParameterGroupName": "string",
      "ParameterApplyStatus": "string"
    }],
    "DbSecurityGroups": ["string"],
    "DbSubnetGroup": {
      "DbSubnetGroupArn": "string",
      "DbSubnetGroupDescription": "string",

```

```
"DbSubnetGroupName": "string",
"SubnetGroupStatus": "string",
"Subnets": [{
  "SubnetAvailabilityZone": {
    "Name": "string"
  },
  "SubnetIdentifier": "string",
  "SubnetStatus": "string"
}],
"VpcId": "string"
},
"DeletionProtection": boolean,
"Endpoint": {
  "Address": "string",
  "Port": number,
  "HostedZoneId": "string"
},
"DomainMemberships": [{
  "Domain": "string",
  "Fqdn": "string",
  "IamRoleName": "string",
  "Status": "string"
}],
"EnabledCloudwatchLogsExports": ["string"],
"Engine": "string",
"EngineVersion": "string",
"EnhancedMonitoringResourceArn": "string",
"IAMDatabaseAuthenticationEnabled": boolean,
"InstanceCreateTime": "string",
"Iops": number,
"KmsKeyId": "string",
"LatestRestorableTime": "string",
"LicenseModel": "string",
"ListenerEndpoint": {
  "Address": "string",
  "HostedZoneId": "string",
  "Port": number
},
"MasterUsername": "admin",
"MaxAllocatedStorage": number,
"MonitoringInterval": number,
"MonitoringRoleArn": "string",
"MultiAz": boolean,
"OptionGroupMemberships": [{
```

```

    "OptionGroupName": "string",
    "Status": "string"
  }],
  "PendingModifiedValues": {
    "AllocatedStorage": number,
    "BackupRetentionPeriod": number,
    "CaCertificateIdentifier": "string",
    "DbInstanceClass": "string",
    "DbInstanceIdentifier": "string",
    "DbSubnetGroupName": "string",
    "EngineVersion": "string",
    "Iops": number,
    "LicenseModel": "string",
    "MasterUserPassword": "string",
    "MultiAZ": boolean,
    "PendingCloudWatchLogsExports": {
      "LogTypesToDisable": ["string"],
      "LogTypesToEnable": ["string"]
    },
    "Port": number,
    "ProcessorFeatures": [{
      "Name": "string",
      "Value": "string"
    }],
    "StorageType": "string"
  },
  "PerformanceInsightsEnabled": boolean,
  "PerformanceInsightsKmsKeyId": "string",
  "PerformanceInsightsRetentionPeriod": number,
  "PreferredBackupWindow": "string",
  "PreferredMaintenanceWindow": "string",
  "ProcessorFeatures": [{
    "Name": "string",
    "Value": "string"
  }],
  "PromotionTier": number,
  "PubliclyAccessible": boolean,
  "ReadReplicaDBClusterIdentifiers": ["string"],
  "ReadReplicaDBInstanceIdentifiers": ["string"],
  "ReadReplicaSourceDBInstanceIdentifier": "string",
  "SecondaryAvailabilityZone": "string",
  "StatusInfos": [{
    "Message": "string",
    "Normal": boolean,

```

```

    "Status": "string",
    "StatusType": "string"
  ]],
  "StorageEncrypted": boolean,
  "TdeCredentialArn": "string",
  "Timezone": "string",
  "VpcSecurityGroups": [{
    "VpcSecurityGroupId": "string",
    "Status": "string"
  }]
},
"AwsRdsDbSecurityGroup": {
  "DbSecurityGroupArn": "string",
  "DbSecurityGroupDescription": "string",
  "DbSecurityGroupName": "string",
  "Ec2SecurityGroups": [{
    "Ec2SecurityGroupArn": "string",
    "Ec2SecurityGroupName": "string",
    "Ec2SecurityGroupOwnerId": "string",
    "Status": "string"
  ]],
  "IpRanges": [{
    "CidrIp": "string",
    "Status": "string"
  }],
  "OwnerId": "string",
  "VpcId": "string"
},
"AwsRdsDbSnapshot": {
  "AllocatedStorage": integer,
  "AvailabilityZone": "string",
  "DbInstanceIdentifier": "string",
  "DbiResourceId": "string",
  "DbSnapshotIdentifier": "string",
  "Encrypted": boolean,
  "Engine": "string",
  "EngineVersion": "string",
  "IamDatabaseAuthenticationEnabled": boolean,
  "InstanceCreateTime": "string",
  "Iops": number,
  "KmsKeyId": "string",
  "LicenseModel": "string",
  "MasterUsername": "string",
  "OptionGroupName": "string",

```

```

    "PercentProgress": integer,
    "Port": integer,
    "ProcessorFeatures": [],
    "SnapshotCreateTime": "string",
    "SnapshotType": "string",
    "SourceDbSnapshotIdentifier": "string",
    "SourceRegion": "string",
    "Status": "string",
    "StorageType": "string",
    "TdeCredentialArn": "string",
    "Timezone": "string",
    "VpcId": "string"
  },
  "AwsRdsEventSubscription": {
    "CustomerAwsId": "string",
    "CustSubscriptionId": "string",
    "Enabled": boolean,
    "EventCategoriesList": ["string"],
    "EventSubscriptionArn": "string",
    "SnsTopicArn": "string",
    "SourceIdsList": ["string"],
    "SourceType": "string",
    "Status": "string",
    "SubscriptionCreationTime": "string"
  },
  "AwsRedshiftCluster": {
    "AllowVersionUpgrade": boolean,
    "AutomatedSnapshotRetentionPeriod": number,
    "AvailabilityZone": "string",
    "ClusterAvailabilityStatus": "string",
    "ClusterCreateTime": "string",
    "ClusterIdentifier": "string",
    "ClusterNodes": [{
      "NodeRole": "string",
      "PrivateIpAddress": "string",
      "PublicIpAddress": "string"
    }],
    "ClusterParameterGroups": [{
      "ClusterParameterStatusList": [{
        "ParameterApplyErrorDescription": "string",
        "ParameterApplyStatus": "string",
        "ParameterName": "string"
      }],
      "ParameterApplyStatus": "string",

```

```

    "ParameterGroupName": "string"
  }],
  "ClusterPublicKey": "string",
  "ClusterRevisionNumber": "string",
  "ClusterSecurityGroups": [{
    "ClusterSecurityGroupName": "string",
    "Status": "string"
  }],
  "ClusterSnapshotCopyStatus": {
    "DestinationRegion": "string",
    "ManualSnapshotRetentionPeriod": number,
    "RetentionPeriod": number,
    "SnapshotCopyGrantName": "string"
  },
  "ClusterStatus": "string",
  "ClusterSubnetGroupName": "string",
  "ClusterVersion": "string",
  "DBName": "string",
  "DeferredMaintenanceWindows": [{
    "DeferMaintenanceEndTime": "string",
    "DeferMaintenanceIdentifier": "string",
    "DeferMaintenanceStartTime": "string"
  }],
  "ElasticIpStatus": {
    "ElasticIp": "string",
    "Status": "string"
  },
  "ElasticResizeNumberOfNodeOptions": "string",
  "Encrypted": boolean,
  "Endpoint": {
    "Address": "string",
    "Port": number
  },
  "EnhancedVpcRouting": boolean,
  "ExpectedNextSnapshotScheduleTime": "string",
  "ExpectedNextSnapshotScheduleTimeStatus": "string",
  "HsmStatus": {
    "HsmClientCertificateIdentifier": "string",
    "HsmConfigurationIdentifier": "string",
    "Status": "string"
  },
  "IamRoles": [{
    "ApplyStatus": "string",
    "IamRoleArn": "string"
  }],

```

```

    }],
    "KmsKeyId": "string",
    "LoggingStatus": {
        "BucketName": "string",
        "LastFailureMessage": "string",
        "LastFailureTime": "string",
        "LastSuccessfulDeliveryTime": "string",
        "LoggingEnabled": boolean,
        "S3KeyPrefix": "string"
    },
    "MaintenanceTrackName": "string",
    "ManualSnapshotRetentionPeriod": number,
    "MasterUsername": "string",
    "NextMaintenanceWindowStartTime": "string",
    "NodeType": "string",
    "NumberOfNodes": number,
    "PendingActions": ["string"],
    "PendingModifiedValues": {
        "AutomatedSnapshotRetentionPeriod": number,
        "ClusterIdentifier": "string",
        "ClusterType": "string",
        "ClusterVersion": "string",
        "EncryptionType": "string",
        "EnhancedVpcRouting": boolean,
        "MaintenanceTrackName": "string",
        "MasterUserPassword": "string",
        "NodeType": "string",
        "NumberOfNodes": number,
        "PubliclyAccessible": "string"
    },
    "PreferredMaintenanceWindow": "string",
    "PubliclyAccessible": boolean,
    "ResizeInfo": {
        "AllowCancelResize": boolean,
        "ResizeType": "string"
    },
    "RestoreStatus": {
        "CurrentRestoreRateInMegabytesPerSecond": number,
        "ElapsedTimeInSeconds": number,
        "EstimatedTimeToCompletionInSeconds": number,
        "ProgressInMegabytes": number,
        "SnapshotSizeInMegabytes": number,
        "Status": "string"
    },
    },

```

```

    "SnapshotScheduleIdentifier": "string",
    "SnapshotScheduleState": "string",
    "VpcId": "string",
    "VpcSecurityGroups": [{
      "Status": "string",
      "VpcSecurityGroupId": "string"
    }]
  },
  "AwsRoute53HostedZone": {
    "HostedZone": {
      "Id": "string",
      "Name": "string",
      "Config": {
        "Comment": "string"
      }
    },
    "NameServers": ["string"],
    "QueryLoggingConfig": {
      "CloudWatchLogsLogGroupArn": {
        "CloudWatchLogsLogGroupArn": "string",
        "Id": "string",
        "HostedZoneId": "string"
      }
    },
    "Vpcs": [
      {
        "Id": "string",
        "Region": "string"
      }
    ]
  },
  "AwsS3AccessPoint": {
    "AccessPointArn": "string",
    "Alias": "string",
    "Bucket": "string",
    "BucketAccountId": "string",
    "Name": "string",
    "NetworkOrigin": "string",
    "PublicAccessBlockConfiguration": {
      "BlockPublicAcls": boolean,
      "BlockPublicPolicy": boolean,
      "IgnorePublicAcls": boolean,
      "RestrictPublicBuckets": boolean
    }
  },

```



```

    "VpcConfiguration": {
      "VpcId": "string"
    }
  },
  "AwsS3AccountPublicAccessBlock": {
    "BlockPublicAcls": boolean,
    "BlockPublicPolicy": boolean,
    "IgnorePublicAcls": boolean,
    "RestrictPublicBuckets": boolean
  },
  "AwsS3Bucket": {
    "AccessControlList": "string",
    "BucketLifecycleConfiguration": {
      "Rules": [{
        "AbortIncompleteMultipartUpload": {
          "DaysAfterInitiation": number
        },
        "ExpirationDate": "string",
        "ExpirationInDays": number,
        "ExpiredObjectDeleteMarker": boolean,
        "Filter": {
          "Predicate": {
            "Operands": [{
              "Prefix": "string",
              "Type": "string"
            },
            {
              "Tag": {
                "Key": "string",
                "Value": "string"
              },
              "Type": "string"
            }
          ],
          "Type": "string"
        }
      }],
      "Id": "string",
      "NoncurrentVersionExpirationInDays": number,
      "NoncurrentVersionTransitions": [{
        "Days": number,
        "StorageClass": "string"
      }],
      "Prefix": "string",

```

```
    "Status": "string",
    "Transitions": [{
      "Date": "string",
      "Days": number,
      "StorageClass": "string"
    }]
  }]
},
"BucketLoggingConfiguration": {
  "DestinationBucketName": "string",
  "LogFilePrefix": "string"
},
"BucketName": "string",
"BucketNotificationConfiguration": {
  "Configurations": [{
    "Destination": "string",
    "Events": ["string"],
    "Filter": {
      "S3KeyFilter": {
        "FilterRules": [{
          "Name": "string",
          "Value": "string"
        }]
      }
    }
  ]},
  "Type": "string"
}],
"BucketVersioningConfiguration": {
  "IsMfaDeleteEnabled": boolean,
  "Status": "string"
},
"BucketWebsiteConfiguration": {
  "ErrorDocument": "string",
  "IndexDocumentSuffix": "string",
  "RedirectAllRequestsTo": {
    "HostName": "string",
    "Protocol": "string"
  },
  "RoutingRules": [{
    "Condition": {
      "HttpErrorCodeReturnedEquals": "string",
      "KeyPrefixEquals": "string"
    }
  ]},
```

```

    "Redirect": {
      "HostName": "string",
      "HttpRedirectCode": "string",
      "Protocol": "string",
      "ReplaceKeyPrefixWith": "string",
      "ReplaceKeyWith": "string"
    }
  ]
},
"CreatedAt": "string",
"ObjectLockConfiguration": {
  "ObjectLockEnabled": "string",
  "Rule": {
    "DefaultRetention": {
      "Days": integer,
      "Mode": "string",
      "Years": integer
    }
  }
},
"OwnerAccountId": "string",
"OwnerId": "string",
"OwnerName": "string",
"PublicAccessBlockConfiguration": {
  "BlockPublicAcls": boolean,
  "BlockPublicPolicy": boolean,
  "IgnorePublicAcls": boolean,
  "RestrictPublicBuckets": boolean
},
"ServerSideEncryptionConfiguration": {
  "Rules": [{
    "ApplyServerSideEncryptionByDefault": {
      "KMSEMasterKeyID": "string",
      "SSEAlgorithm": "string"
    }
  ]
}
},
"awsS3Object": {
  "ContentType": "string",
  "ETag": "string",
  "LastModified": "string",
  "ServerSideEncryption": "string",
  "SSEKMSKeyId": "string",

```

```

    "VersionId": "string"
  },
  "AwsSagemakerNotebookInstance": {
    "DirectInternetAccess": "string",
    "InstanceMetadataServiceConfiguration": {
      "MinimumInstanceMetadataServiceVersion": "string"
    },
    "InstanceType": "string",
    "LastModifiedTime": "string",
    "NetworkInterfaceId": "string",
    "NotebookInstanceArn": "string",
    "NotebookInstanceName": "string",
    "NotebookInstanceStatus": "string",
    "PlatformIdentifier": "string",
    "RoleArn": "string",
    "RootAccess": "string",
    "SecurityGroups": ["string"],
    "SubnetId": "string",
    "Url": "string",
    "VolumeSizeInGB": number
  },
  "AwsSecretsManagerSecret": {
    "Deleted": boolean,
    "Description": "string",
    "KmsKeyId": "string",
    "Name": "string",
    "RotationEnabled": boolean,
    "RotationLambdaArn": "string",
    "RotationOccurredWithinFrequency": boolean,
    "RotationRules": {
      "AutomaticallyAfterDays": integer
    }
  },
  "AwsSnsTopic": {
    "ApplicationSuccessFeedbackRoleArn": "string",
    "FirehoseFailureFeedbackRoleArn": "string",
    "FirehoseSuccessFeedbackRoleArn": "string",
    "HttpFailureFeedbackRoleArn": "string",
    "HttpSuccessFeedbackRoleArn": "string",
    "KmsMasterKeyId": "string",
    "Owner": "string",
    "SqsFailureFeedbackRoleArn": "string",
    "SqsSuccessFeedbackRoleArn": "string",
    "Subscription": {

```

```
    "Endpoint": "string",
    "Protocol": "string"
  },
  "TopicName": "string"
},
"AwsSqsQueue": {
  "DeadLetterTargetArn": "string",
  "KmsDataKeyReusePeriodSeconds": number,
  "KmsMasterKeyId": "string",
  "QueueName": "string"
},
"AwsSsmPatchCompliance": {
  "Patch": {
    "ComplianceSummary": {
      "ComplianceType": "string",
      "CompliantCriticalCount": integer,
      "CompliantHighCount": integer,
      "CompliantInformationalCount": integer,
      "CompliantLowCount": integer,
      "CompliantMediumCount": integer,
      "CompliantUnspecifiedCount": integer,
      "ExecutionType": "string",
      "NonCompliantCriticalCount": integer,
      "NonCompliantHighCount": integer,
      "NonCompliantInformationalCount": integer,
      "NonCompliantLowCount": integer,
      "NonCompliantMediumCount": integer,
      "NonCompliantUnspecifiedCount": integer,
      "OverallSeverity": "string",
      "PatchBaselineId": "string",
      "PatchGroup": "string",
      "Status": "string"
    }
  }
},
"AwsStepFunctionStateMachine": {
  "StateMachineArn": "string",
  "Name": "string",
  "Status": "string",
  "RoleArn": "string",
  "Type": "string",
  "LoggingConfiguration": {
    "Level": "string",
    "IncludeExecutionData": boolean
  }
}
```

```

    },
    "TracingConfiguration": {
      "Enabled": boolean
    }
  },
  "AwsWafRateBasedRule": {
    "MatchPredicates": [{
      "DataId": "string",
      "Negated": boolean,
      "Type": "string"
    }],
    "MetricName": "string",
    "Name": "string",
    "RateKey": "string",
    "RateLimit": number,
    "RuleId": "string"
  },
  "AwsWafRegionalRateBasedRule": {
    "MatchPredicates": [{
      "DataId": "string",
      "Negated": boolean,
      "Type": "string"
    }],
    "MetricName": "string",
    "Name": "string",
    "RateKey": "string",
    "RateLimit": number,
    "RuleId": "string"
  },
  "AwsWafRegionalRule": {
    "MetricName": "string",
    "Name": "string",
    "RuleId": "string",
    "PredicateList": [{
      "DataId": "string",
      "Negated": boolean,
      "Type": "string"
    }]
  },
  "AwsWafRegionalRuleGroup": {
    "MetricName": "string",
    "Name": "string",
    "RuleGroupId": "string",
    "Rules": [{

```

```

    "Action": {
      "Type": "string"
    },
    "Priority": number,
    "RuleId": "string",
    "Type": "string"
  ]
},
"AwsWafRegionalWebAcl": {
  "DefaultAction": "string",
  "MetricName": "string",
  "Name": "string",
  "RulesList": [{
    "Action": {
      "Type": "string"
    },
    "Priority": number,
    "RuleId": "string",
    "Type": "string",
    "ExcludedRules": [{
      "ExclusionType": "string",
      "RuleId": "string"
    }],
    "OverrideAction": {
      "Type": "string"
    }
  ]},
  "WebAclId": "string"
},
"AwsWafRule": {
  "MetricName": "string",
  "Name": "string",
  "PredicateList": [{
    "DataId": "string",
    "Negated": boolean,
    "Type": "string"
  ]},
  "RuleId": "string"
},
"AwsWafRuleGroup": {
  "MetricName": "string",
  "Name": "string",
  "RuleGroupId": "string",
  "Rules": [{

```

```

    "Action": {
      "Type": "string"
    },
    "Priority": number,
    "RuleId": "string",
    "Type": "string"
  ]]
},
"AwsWafv2RuleGroup": {
  "Arn": "string",
  "Capacity": number,
  "Description": "string",
  "Id": "string",
  "Name": "string",
  "Rules": [{
    "Action": {
      "Allow": {
        "CustomRequestHandling": {
          "InsertHeaders": [
            {
              "Name": "string",
              "Value": "string"
            },
            {
              "Name": "string",
              "Value": "string"
            }
          ]
        }
      }
    },
    "Name": "string",
    "Priority": number,
    "VisibilityConfig": {
      "CloudWatchMetricsEnabled": boolean,
      "MetricName": "string",
      "SampledRequestsEnabled": boolean
    }
  }],
  "VisibilityConfig": {
    "CloudWatchMetricsEnabled": boolean,
    "MetricName": "string",
    "SampledRequestsEnabled": boolean
  }
}

```



```

},
"AwsWafWebAcl": {
  "DefaultAction": "string",
  "Name": "string",
  "Rules": [{
    "Action": {
      "Type": "string"
    },
    "ExcludedRules": [{
      "RuleId": "string"
    }],
    "OverrideAction": {
      "Type": "string"
    },
    "Priority": number,
    "RuleId": "string",
    "Type": "string"
  }],
  "WebAclId": "string"
},
"AwsWafv2WebAcl": {
  "Arn": "string",
  "Capacity": number,
  "CaptchaConfig": {
    "ImmunityTimeProperty": {
      "ImmunityTime": number
    }
  },
  "DefaultAction": {
    "Block": {}
  },
  "Description": "string",
  "ManagedbyFirewallManager": boolean,
  "Name": "string",
  "Rules": [{
    "Action": {
      "RuleAction": {
        "Block": {}
      }
    },
    "Name": "string",
    "Priority": number,
    "VisibilityConfig": {
      "SampledRequestsEnabled": boolean,

```

```

    "CloudWatchMetricsEnabled": boolean,
    "MetricName": "string"
  }
}],
"VisibilityConfig": {
  "SampledRequestsEnabled": boolean,
  "CloudWatchMetricsEnabled": boolean,
  "MetricName": "string"
},
"AwsXrayEncryptionConfig": {
  "KeyId": "string",
  "Status": "string",
  "Type": "string"
},
"Container": {
  "ContainerRuntime": "string",
  "ImageId": "string",
  "ImageName": "string",
  "LaunchedAt": "string",
  "Name": "string",
  "Privileged": boolean,
  "VolumeMounts": [{
    "Name": "string",
    "MountPath": "string"
  }]
},
"Other": {
  "string": "string"
},
"Id": "string",
"Partition": "string",
"Region": "string",
"ResourceRole": "string",
"Tags": {
  "string": "string"
},
"Type": "string"
}],
"SchemaVersion": "string",
"Severity": {
  "Label": "string",
  "Normalized": number,
  "Original": "string"
}

```

```

},
"Sample": boolean,
"SourceUrl": "string",
"Threats": [{
  "FilePaths": [{
    "FileName": "string",
    "FilePath": "string",
    "Hash": "string",
    "ResourceId": "string"
  }],
  "ItemCount": number,
  "Name": "string",
  "Severity": "string"
}],
"ThreatIntelIndicators": [{
  "Category": "string",
  "LastObservedAt": "string",
  "Source": "string",
  "SourceUrl": "string",
  "Type": "string",
  "Value": "string"
}],
"Title": "string",
"Types": ["string"],
"UpdatedAt": "string",
"UserDefinedFields": {
  "string": "string"
},
"VerificationState": "string",
"Vulnerabilities": [{
  "CodeVulnerabilities": [{
    "Cwes": [
      "string",
      "string"
    ],
    "FilePath": {
      "EndLine": integer,
      "FileName": "string",
      "FilePath": "string",
      "StartLine": integer
    },
    "SourceArn": "string"
  }],
  "Cvss": [{

```

```

    "Adjustments": [{
      "Metric": "string",
      "Reason": "string"
    }],
    "BaseScore": number,
    "BaseVector": "string",
    "Source": "string",
    "Version": "string"
  }],
  "EpssScore": number,
  "ExploitAvailable": "string",
  "FixAvailable": "string",
  "Id": "string",
  "LastKnownExploitAt": "string",
  "ReferenceUrls": ["string"],
  "RelatedVulnerabilities": ["string"],
  "Vendor": {
    "Name": "string",
    "Url": "string",
    "VendorCreatedAt": "string",
    "VendorSeverity": "string",
    "VendorUpdatedAt": "string"
  },
  "VulnerablePackages": [{
    "Architecture": "string",
    "Epoch": "string",
    "FilePath": "string",
    "FixedInVersion": "string",
    "Name": "string",
    "PackageManager": "string",
    "Release": "string",
    "Remediation": "string",
    "SourceLayerArn": "string",
    "SourceLayerHash": "string",
    "Version": "string"
  }]
}],
  "Workflow": {
    "Status": "string"
  },
  "WorkflowState": "string"
}
]

```

Auswirkungen der Konsolidierung auf ASFF-Felder und -Werte

AWS Security Hub Cloud Security Posture Management (CSPM) bietet zwei Arten der Konsolidierung von Kontrollen:

- **Ansicht konsolidierter Kontrollen** — Bei dieser Art der Konsolidierung hat jede Kontrolle eine einzige Kennung für alle Standards. Darüber hinaus werden auf der Security Hub CSPM-Konsole auf der Seite „Kontrollen“ alle Kontrollen für alle Standards angezeigt.
- **Konsolidierte Kontrollergebnisse** — Bei dieser Art der Konsolidierung liefert Security Hub CSPM ein einziges Ergebnis für eine Kontrolle, auch wenn die Kontrolle für mehrere aktivierte Standards gilt. Dadurch kann das Störgeräusch beim Auffinden reduziert werden.

Sie können die Ansicht der konsolidierten Steuerelemente nicht aktivieren oder deaktivieren. Consolidated Control Findings ist standardmäßig aktiviert, wenn Sie Security Hub CSPM am oder nach dem 23. Februar 2023 aktivieren. Andernfalls ist es standardmäßig deaktiviert. Für Unternehmen ist Consolidated Control Findings jedoch nur für Security Hub CSPM-Mitgliedskonten aktiviert, wenn sie für das Administratorkonto aktiviert sind. Weitere Informationen zu konsolidierten Kontrollergebnissen finden Sie unter [Generierung und Aktualisierung von Kontrollbefunden](#)

Beide Konsolidierungsarten wirken sich auf Felder und Werte für Kontrollergebnisse in der aus [AWS Format für Sicherheitssuche \(ASFF\)](#).

Themen

- [Ansicht konsolidierter Kontrollen — ASFF-Änderungen](#)
- [Konsolidierte Kontrollergebnisse — ASFF-Änderungen](#)
- [Generator IDs vor und nach der Aktivierung konsolidierter Kontrollergebnisse](#)
- [Wie sich die Konsolidierung auf Kontrolle und Titel auswirkt IDs](#)
- [Aktualisierung der Workflows für die Konsolidierung](#)

Ansicht konsolidierter Kontrollen — ASFF-Änderungen

Mit der Funktion zur Ansicht konsolidierter Kontrollen wurden die folgenden Änderungen an Feldern und Werten für Kontrollergebnisse in der ASFF eingeführt. Wenn Ihre Workflows nicht auf Werten für diese ASFF-Felder basieren, sind keine Maßnahmen erforderlich. Wenn Sie Workflows haben, die auf bestimmten Werten für diese Felder basieren, aktualisieren Sie Ihre Workflows, sodass sie die aktuellen Werte verwenden.

ASFF-Feld	Beispielwert vor Ansicht der konsolidierten Kontrollen	Beispielwert nach Ansicht der konsolidierten Kontrollen und Beschreibung der Änderung
Einhaltung der Vorschriften. SecurityControlId	Nicht zutreffend (neues Feld)	EC22. Führt eine einzige Kontroll-ID für alle Standards ein. ProductFields.RuleId stellt weiterhin die standardbasierte Kontroll-ID für CIS v1.2.0-Steurelemente bereit. ProductFields.ControlId stellt weiterhin die standardbasierte Kontroll-ID für Steuerungen in anderen Standards bereit.
Einhaltung der Vorschriften. AssociatedStandards	Nicht zutreffend (neues Feld)	[{"StandardId": "aws-foundational-security-best-practices/v1.0.0"}] Zeigt an, in welchen Standards ein Steuerelement aktiviert ist.
ProductFields.ArchivalReasons. -----SEP-----:0/Beschreibung	Nicht zutreffend (neues Feld)	„Das Ergebnis befindet sich im Status ARCHIVIERT, da konsolidierte Kontrollegebnisse aktiviert oder deaktiviert wurden. Dies führt dazu, dass Ergebnisse im vorherigen Status archiviert werden, wenn neue Ergebnisse generiert werden.“

ASFF-Feld	Beispielwert vor Ansicht der konsolidierten Kontrollen	Beispielwert nach Ansicht der konsolidierten Kontrollen und Beschreibung der Änderung
		Beschreibt, warum Security Hub CSPM bestehende Ergebnisse archiviert hat.
ProductFields.ArchivalReasons. ----sep----:0/ReasonCode	Nicht zutreffend (neues Feld)	„CONSOLIDATED_CONTROL_FINDINGS_UPDATE“ Liefert den Grund, warum Security Hub CSPM bestehende Ergebnisse archiviert hat.
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation Dieses Feld verweist nicht mehr auf einen Standard.
Abhilfe.Empfehlung.Text	„Anweisungen zur Behebung dieses Problems finden Sie in der PCI DSS-Dokumentation zu AWS Security Hub Cloud Security Posture Management (CSPM).“	„Anweisungen zur Behebung dieses Problems finden Sie in der Dokumentation zu AWS Security Hub Cloud Security Posture Management (CSPM) Controls.“ Dieses Feld verweist nicht mehr auf einen Standard.
Abhilfe.Empfehlung.Url	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation Dieses Feld verweist nicht mehr auf einen Standard.

Konsolidierte Kontrollergebnisse — ASFF-Änderungen

Wenn Sie konsolidierte Kontrollergebnisse aktivieren, sind Sie möglicherweise von den folgenden Änderungen an Feldern und Werten für Kontrollergebnisse im ASFF betroffen. Diese Änderungen kommen zu den Änderungen hinzu, die durch die Funktion zur Ansicht konsolidierter Kontrollen eingeführt wurden. Wenn Ihre Workflows nicht auf Werten für diese ASFF-Felder basieren, sind keine Maßnahmen erforderlich. Wenn Sie Workflows haben, die auf bestimmten Werten für diese Felder basieren, aktualisieren Sie Ihre Workflows, sodass sie die aktuellen Werte verwenden.

Tip

Wenn Sie die Lösung [Automated Security Response auf AWS Version 2.0.0](#) verwenden, beachten Sie, dass sie konsolidierte Kontrollergebnisse unterstützt. Das bedeutet, dass Sie Ihre aktuellen Workflows beibehalten können, wenn Sie konsolidierte Kontrollergebnisse aktivieren.

ASFF-Feld	Beispielwert vor der Aktivierung konsolidierter Kontrollergebnisse	Beispielwert nach der Aktivierung konsolidierter Kontrollergebnisse und Beschreibung der Änderung
GeneratorId	aws-foundational-security-best-practices/v/1.0.0/Config 1.	Sicherheitskontrolle/Config.1 Dieses Feld verweist nicht mehr auf einen Standard.
Title	AWS Config PCI.Config.1 sollte aktiviert sein	AWS Config sollte aktiviert sein Dieses Feld verweist nicht mehr auf standardspezifische Informationen.
Id	arn:aws:securityhub:eu-central-1:123456789012:6d6a26-a156-48f0-9403-115983e5a956 subscription/pci-dss/v/3.2.1/PCI.IAM.5/finding/ab	arn:aws:securityhub:eu-central-1:123456789012:security-6d6a26-a156-48f0-9403-115983e5a956 control/iam.9/finding/ab

ASFF-Feld	Beispielwert vor der Aktivierung konsolidierter Kontrollergebnisse	Beispielwert nach der Aktivierung konsolidierter Kontrollergebnisse und Beschreibung der Änderung
		Dieses Feld verweist nicht mehr auf einen Standard.
ProductFields.ControlId	PCI. EC22.	Entfernt. Siehe Compliance.SecurityControlId stattdessen. Dieses Feld wurde zugunsten einer einzigen, standardunabhängigen Kontroll-ID entfernt.
ProductFields.RuleId	1.3	Entfernt. Siehe Compliance.SecurityControlId stattdessen. Dieses Feld wurde zugunsten einer einzigen, standardunabhängigen Kontroll-ID entfernt.
Beschreibung	Diese PCI-DSS-Steuerung prüft, ob sie im Girokonto und in der Region aktiviert AWS Config ist.	Diese AWS Kontrolle prüft, ob sie im Girokonto und in der Region aktiviert AWS Config ist. Dieses Feld verweist nicht mehr auf einen Standard.

ASFF-Feld	Beispielwert vor der Aktivierung konsolidierter Kontrollergebnisse	Beispielwert nach der Aktivierung konsolidierter Kontrollergebnisse und Beschreibung der Änderung
Schweregrad	<pre>„Schweregrad“: { „Produkt“: 90, „Label“: „KRITISCH“, „Normalisiert“: 90, „Original“: „KRITISCH“ }</pre>	<pre>„Schweregrad“: { „Label“: „KRITISCH“, „Normalisiert“: 90, „Original“: „KRITISCH“ }</pre> Security Hub CSPM verwendet das Feld Produkt nicht mehr, um den Schweregrad eines Fehlers zu beschreiben.
Typen	["Software Checks/Industry und Konfiguration sowie behördliche Standards/PCI-DSS"]	["Software und Konfiguration sowie regulatorische Standards"] Checks/Industry Dieses Feld verweist nicht mehr auf einen Standard.
Einhaltung. RelatedRequirements	["PCI DSS 10.5.2“, „PCI DSS 11.5“, „CIS AWS Foundations 2.5"]	["PCI DSS v3.2.1/10.5.2“, „PCI DSS v3.2.1/11,5“, „Benchmark v1.2.0/2.5" der CIS Foundations] AWS In diesem Feld werden die entsprechenden Anforderungen in allen aktivierten Standards angezeigt.

ASFF-Feld	Beispielwert vor der Aktivierung konsolidierter Kontrollergebnisse	Beispielwert nach der Aktivierung konsolidierter Kontrollergebnisse und Beschreibung der Änderung
CreatedAt	2015-05-05T 08:18:13.138 Z	25.09.2022 08:18:13,138 Z Das Format bleibt unverändert, aber der Wert wird zurückgesetzt, wenn Sie konsolidierte Kontrolle rgebnisse aktivieren.
FirstObservedAt	07.05.2022 08:18:13.138 Z	28.09.2022 08:18:13.138 Z Das Format bleibt unverändert, aber der Wert wird zurückgesetzt, wenn Sie konsolidierte Kontrolle rgebnisse aktivieren.
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation	Entfernt. Siehe Remediation.Recommendation.Url stattdessen.
ProductFields.StandardsArn	arn:aws:securityhub:::/1.0.0/standards/aws-foundational-security-best-practices/v	Entfernt. Siehe Compliance.AssociatedStandards stattdessen.
ProductFields.StandardsControlArn	arn:aws:securityhub:us-east-1:123456789012:/1.0.0/control/aws-foundational-security-best-practices/v/1.0.0/Config	Entfernt. Security Hub CSPM generiert ein Ergebnis für eine standardübergreifende Sicherheitsüberprüfung.
ProductFields.StandardsGuideArn	arn:aws:securityhub:::/1.2.0/ruleset/cis-aws-foundations-benchmark/v	Entfernt. Siehe Compliance.AssociatedStandards stattdessen.
ProductFields.StandardsGuideSubscriptionArn	arn:aws:securityhub:us-east-2:123456789012:/1.2.0/subscription/cis-aws-foundations-benchmark/v	Entfernt. Security Hub CSPM generiert ein Ergebnis für eine standardübergreifende Sicherheitsüberprüfung.

ASFF-Feld	Beispielwert vor der Aktivierung konsolidierter Kontrollergebnisse	Beispielwert nach der Aktivierung konsolidierter Kontrollergebnisse und Beschreibung der Änderung
ProductFields.StandardsSubscriptionArn	arn:aws:securityhub:us-east-1:123456789012:/1.0.0 subscription/aws-foundational-security-best-practices/v	Entfernt. Security Hub CSPM generiert ein Ergebnis für eine standardübergreifende Sicherheitsüberprüfung.
ProductFields.aws/securityhub/FindingId	arn:aws:securityhub:us-east-1::/751c2173-7372-4e12-8656-a5210dfb1d67 product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0/Config.1/finding	arn:aws:securityhub:us-east-1::/751c2173-7372-4e12-8656-a5210dfb1d67 product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:security-control/Config.1/finding Dieses Feld verweist nicht mehr auf einen Standard.

Werte für vom Kunden bereitgestellte ASFF-Felder nach Aktivierung der konsolidierten Kontrollergebnisse

Wenn Sie konsolidierte Kontrollergebnisse aktivieren, generiert Security Hub CSPM ein standardübergreifendes Ergebnis und archiviert die ursprünglichen Ergebnisse (separate Ergebnisse für jeden Standard).

Aktualisierungen, die Sie mit der Security Hub CSPM-Konsole oder dem [BatchUpdateFindings](#) Vorgang an den ursprünglichen Ergebnissen vorgenommen haben, werden in den neuen Ergebnissen nicht beibehalten. Bei Bedarf können Sie diese Daten wiederherstellen, indem Sie auf die archivierten Ergebnisse zurückgreifen. Um archivierte Ergebnisse zu überprüfen, können Sie die Seite Ergebnisse in der Security Hub CSPM-Konsole verwenden und den Filter Datensatzstatus auf ARCHIVIERT setzen. Alternativ können Sie den [GetFindings](#) Betrieb der Security Hub CSPM-API verwenden.

Vom Kunden bereitgestelltes ASFF-Feld	Beschreibung der Änderung nach der Aktivierung der konsolidierten Kontrollergebnisse
Wahrscheinlichkeit	Setzt auf den leeren Zustand zurück.
Kritikalität	Setzt auf den leeren Zustand zurück.
Hinweis	Setzt auf den leeren Zustand zurück.
RelatedFindings	Setzt auf den leeren Zustand zurück.
Schweregrad	Standardschweregrad des Ergebnisses (entspricht dem Schweregrad der Kontrolle).
Typen	Wird auf den standardunabhängigen Wert zurückgesetzt.
UserDefinedFields	Setzt auf den leeren Zustand zurück.
VerificationState	Setzt auf den leeren Zustand zurück.
Workflow	Neue fehlgeschlagene Ergebnisse haben einen Standardwert von. NEW Neue bestandene Ergebnisse haben einen Standardwert vonRESOLVED.

Generator IDs vor und nach der Aktivierung konsolidierter Kontrollergebnisse

In der folgenden Tabelle sind Änderungen an den Generator-ID-Werten für Kontrollen aufgeführt, wenn Sie konsolidierte Kontrollergebnisse aktivieren. Diese Änderungen gelten für Kontrollen, die Security Hub CSPM am 15. Februar 2023 unterstützt hat.

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
arn:aws:securityhub:::/1.1 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/ CloudWatch 1.

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
arn:aws:securityhub::: /1.10 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/IAM.16
arn:aws:securityhub::: /1.11 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/IAM.17
arn:aws:securityhub::: /1.12 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/IAM.4
arn:aws:securityhub::: /1.13 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/IAM.9
arn:aws:securityhub::: /1.14 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/IAM.6
arn:aws:securityhub::: /1.16 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/IAM.2
arn:aws:securityhub::: /1.2 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/IAM.5
arn:aws:securityhub::: /1.20 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/IAM.18
arn:aws:securityhub::: /1.22 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/IAM.1
arn:aws:securityhub::: /1.3 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/IAM.8
arn:aws:securityhub::: /1.4 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/IAM.3
arn:aws:securityhub::: /1.5 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/IAM.11

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
arn:aws:securityhub::: /1.6 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/IAM.12
arn:aws:securityhub::: /1.7 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/IAM.13
arn:aws:securityhub::: /1.8 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/IAM.14
arn:aws:securityhub::: /1.9 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/IAM.15
arn:aws:securityhub::: /2.1 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/ CloudTrail 1.
arn:aws:securityhub::: /2.2 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/ CloudTrail .4
arn:aws:securityhub::: /2.3 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/ CloudTrail .6
arn:aws:securityhub::: /2.4 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/ CloudTrail 1.5
arn:aws:securityhub::: /2.5 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/Config.1
arn:aws:securityhub::: /2.6 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/ CloudTrail .7
arn:aws:securityhub::: /2.7 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/ CloudTrail 2.
arn:aws:securityhub::: /2.8 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/KMS.4

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
arn:aws:securityhub:::/2.9 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/ EC2 .6
arn:aws:securityhub:::/3.1 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/ CloudWatch 2.
arn:aws:securityhub:::/3.2 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/ CloudWatch 3.
arn:aws:securityhub:::/3.3 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/ CloudWatch 1.
arn:aws:securityhub:::/3.4 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/ CloudWatch .4
arn:aws:securityhub:::/3.5 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/ CloudWatch 3.5
arn:aws:securityhub:::/3.6 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/ CloudWatch 3.6
arn:aws:securityhub:::/3.7 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/ CloudWatch .7
arn:aws:securityhub:::/3.8 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/. CloudWatch 8
arn:aws:securityhub:::/3.9 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/ CloudWatch .9
arn:aws:securityhub:::/3.10 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/ CloudWatch 1.0
arn:aws:securityhub:::/3.11 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/ CloudWatch .11

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
arn:aws:securityhub:::/3.12 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/ CloudWatch 1.2
arn:aws:securityhub:::/3.13 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/ CloudWatch 1.3
arn:aws:securityhub:::/3.14 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/ CloudWatch 1.4
arn:aws:securityhub:::/4.1 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/ EC2 1.3
arn:aws:securityhub:::/4.2 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/ EC2 1.4
arn:aws:securityhub:::/4.3 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Sicherheitskontrolle/ EC2 2.
cis-aws-foundations-benchmark/v/1.4.0/1.10	Sicherheitskontrolle/IAM.5
cis-aws-foundations-benchmark/v/1.4.0/1.14	Sicherheitskontrolle/IAM.3
cis-aws-foundations-benchmark/v/1.4.0/1.16	Sicherheitskontrolle/IAM.1
cis-aws-foundations-benchmark/v/1.4.0/1.17	Sicherheitskontrolle/IAM.18
cis-aws-foundations-benchmark/v/1.4.0/1.4	Sicherheitskontrolle/IAM.4
cis-aws-foundations-benchmark/v/1.4.0/1.5	Sicherheitskontrolle/IAM.9
cis-aws-foundations-benchmark/v/1.4.0/1.6	Sicherheitskontrolle/IAM.6
cis-aws-foundations-benchmark/v/1.4.0/1.7	Sicherheitskontrolle/ 1. CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/1.8	Sicherheitskontrolle/IAM.15
cis-aws-foundations-benchmark/v/1.4.0/1.9	Sicherheitskontrolle/IAM.16

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
cis-aws-foundations-benchmark/v/1.4.0/2.1.2	Sicherheitskontrolle/S3.5
cis-aws-foundations-benchmark/v/1.4.0/2.1.5.1	Sicherheitskontrolle/S3.1
cis-aws-foundations-benchmark/v/1.4.0/2.1.5.2	Sicherheitskontrolle/S3.8
cis-aws-foundations-benchmark/v/1.4.0/2.2.1	Sicherheitskontrolle/ .7 EC2
cis-aws-foundations-benchmark/v/1.4.0/2.3.1	Sicherheitskontrolle/RDS.3
cis-aws-foundations-benchmark/v/1.4.0/3.1	Sicherheitskontrolle/ 1. CloudTrail
cis-aws-foundations-benchmark/v/1.4.0/3.2	Sicherheitskontrolle/ .4 CloudTrail
cis-aws-foundations-benchmark/v/1.4.0/3.4	Sicherheitskontrolle/ 3.5 CloudTrail
cis-aws-foundations-benchmark/v/1.4.0/3.5	Sicherheitskontrolle/Config.1
cis-aws-foundations-benchmark/v/1.4.0/3.6	Sicherheitskontrolle/S3.9
cis-aws-foundations-benchmark/v/1.4.0/3.7	Sicherheitskontrolle/ .2 CloudTrail
cis-aws-foundations-benchmark/v/1.4.0/3.8	Sicherheitskontrolle/KMS.4
cis-aws-foundations-benchmark/v/1.4.0/3.9	Sicherheitskontrolle/ .6 EC2
cis-aws-foundations-benchmark/v/1.4.0/4.3	Sicherheitskontrolle/ 1. CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.4	Sicherheitskontrolle/ .4 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.5	Sicherheitskontrolle/ 4.5 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.6	Sicherheitskontrolle/ .6 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.7	Sicherheitskontrolle/ .7 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.8	Sicherheitskontrolle/ .8 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.9	Sicherheitskontrolle/ .9 CloudWatch

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
cis-aws-foundations-benchmark/v/1.4.0/4.10	Sicherheitskontrolle/ 1.0 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.11	Sicherheitskontrolle/ 1.1 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.12	Sicherheitskontrolle/ 1.2 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.13	Sicherheitskontrolle/ 1.3 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.14	Sicherheitskontrolle/ 1.4 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/5.1	Sicherheitskontrolle/ 2.1 EC2
cis-aws-foundations-benchmark/v/1.4.0/5.3	Sicherheitskontrolle/ .2 EC2
aws-foundational-security-best-practices/ v/1.0.0/Account 1.	Sicherheitskontrolle/Konto.1
aws-foundational-security-best-practices/ v/1.0.0/ACM	Sicherheitskontrolle/ACM.1
aws-foundational-security-best-practices/ v/1.0.0/APIGateway	Sicherheitskontrolle/ .1 APIGateway
aws-foundational-security-best-practices/ v/1.0.0/APIGateway 2.	Sicherheitskontrolle/ .2 APIGateway
aws-foundational-security-best-practices/ v/1.0.0/APIGateway 3.	Sicherheitskontrolle/ .3 APIGateway
aws-foundational-security-best-practices/ v/1.0.0/APIGateway 4.	Sicherheitskontrolle/ .4 APIGateway
aws-foundational-security-best-practices/v/1. 0.0/APIGateway.	Sicherheitskontrolle/ .5 APIGateway
aws-foundational-security-best-practices/v/1. 0.0/APIGateway.	Sicherheitskontrolle/ .8 APIGateway

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-foundational-security-best-9practices/v/1.0.0/APIGateway.	Sicherheitskontrolle/ .9 APIGateway
aws-foundational-security-best- practices/ v/1.0.0/AutoScaling 1.	Sicherheitskontrolle/ .1 AutoScaling
aws-foundational-security-best- practices/ v/1.0.0/AutoScaling 2.	Sicherheitskontrolle/ .2 AutoScaling
aws-foundational-security-best- practices/ v/1.0.0/AutoScaling 3.	Sicherheitskontrolle/ .3 AutoScaling
aws-foundational-security-best- practices/ v/1.0.0/Autoscaling 5.	Sicherheitskontrolle/Autoscaling.5
aws-foundational-security-best- 6. practices/ v/1.0.0/AutoScaling	Sicherheitskontrolle/ .6 AutoScaling
aws-foundational-security-best- practices/ v/1.0.0/AutoScaling 9.	Sicherheitskontrolle/ .9 AutoScaling
aws-foundational-security-best- practices/ v/1.0.0/CloudFront 1.	Sicherheitskontrolle/ .1 CloudFront
aws-foundational-security-best- practices/ v/1.0.0/CloudFront 3.	Sicherheitskontrolle/ .3 CloudFront
aws-foundational-security-best- practices/ v/1.0.0/CloudFront 4.	Sicherheitskontrolle/ .4 CloudFront
aws-foundational-security-best-practices/v/1.0.0/CloudFront.	Sicherheitskontrolle/ .5 CloudFront
aws-foundational-security-best- practices/ v/1.0.0/CloudFront 6.	Sicherheitskontrolle/ .6 CloudFront

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-foundational-security-best-practices/ v/1.0.0/CloudFront 7.	Sicherheitskontrolle/ .7 CloudFront
aws-foundational-security-best-practices/v/1. 0.0/CloudFront.	Sicherheitskontrolle/ .8 CloudFront
aws-foundational-security-best-9practices/v/1 .0.0/CloudFront.	Sicherheitskontrolle/ .9 CloudFront
aws-foundational-security-best-practices/ v/1.0.0/CloudFront 1,0	Sicherheitskontrolle/ .10 CloudFront
aws-foundational-security-best-practices/ v/1.0.0/CloudFront 1.2	Sicherheitskontrolle/ .12 CloudFront
aws-foundational-security-best-practices/ v/1.0.0/CloudTrail 1.	Sicherheitskontrolle/ .1 CloudTrail
aws-foundational-security-best-practices/ v/1.0.0/CloudTrail 2.	Sicherheitskontrolle/ .2 CloudTrail
aws-foundational-security-best-practices/ v/1.0.0/CloudTrail 4.	Sicherheitskontrolle/ .4 CloudTrail
aws-foundational-security-best-practices/v/1. 0.0/CloudTrail.	Sicherheitskontrolle/ .5 CloudTrail
aws-foundational-security-best-practices/ v/1.0.0/CodeBuild 1.	Sicherheitskontrolle/ .1 CodeBuild
aws-foundational-security-best-practices/ v/1.0.0/CodeBuild 2.	Sicherheitskontrolle/ .2 CodeBuild
aws-foundational-security-best-practices/ v/1.0.0/CodeBuild 3.	Sicherheitskontrolle/ .3 CodeBuild

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-foundational-security-best-practices/ v/1.0.0/CodeBuild 4.	Sicherheitskontrolle/ .4 CodeBuild
aws-foundational-security-best-practices/ v/1.0.0/Config 1.	Sicherheitskontrolle/Config.1
aws-foundational-security-best- 1. practices/ v/1.0.0/DMS	Sicherheitskontrolle/DMS.1
aws-foundational-security-best- 1. practices/ v/1.0.0/DynamoDB	Sicherheitskontrolle/DynamoDB.1
aws-foundational-security-best- 1.2 practices/ v/1.0.0/DynamoDB	Sicherheitskontrolle/DynamoDB.2
aws-foundational-security-best- 3. practices/ v/1.0.0/DynamoDB	Sicherheitskontrolle/DynamoDB.3
aws-foundational-security-best- 2.1 practices/ v/1.0.0/EC	Sicherheitskontrolle/ 1. EC2
aws-foundational-security-best-practices/ v/1.0.0/EC 2,3	Sicherheitskontrolle/ 2.3 EC2
aws-foundational-security-best-practices/ v/1.0.0/EC 2,4	Sicherheitskontrolle/ 4. EC2
aws-foundational-security-best-practices/ v/1.0.0/EC 2,6	Sicherheitskontrolle/ 2.6 EC2
aws-foundational-security-best-practices/ v/1.0.0/EC 2,7	Sicherheitskontrolle/ 7. EC2
aws-foundational-security-best-practices/ v/1.0.0/EC 2,8	Sicherheitskontrolle/. 8 EC2

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-foundational-security-best-practices/ v/1.0.0/EC 2,9	Sicherheitskontrolle/ 9. EC2
aws-foundational-security-best-practices/ v/1.0.0/EC 2,10	Sicherheitskontrolle/ 1.0 EC2
aws-foundational-security-best-practices/ v/1.0.0/EC 2,15	Sicherheitskontrolle/ 1.5 EC2
aws-foundational-security-best-practices/ v/1.0.0/EC 2,16	Sicherheitskontrolle/ 1.6 EC2
aws-foundational-security-best-practices/ v/1.0.0/EC 2,17	Sicherheitskontrolle/ 1.7 EC2
aws-foundational-security-best-practices/ v/1.0.0/EC 2,18	Sicherheitskontrolle/ 1.8 EC2
aws-foundational-security-best-practices/ v/1.0.0/EC 2,19	Sicherheitskontrolle/ 1.9 EC2
aws-foundational-security-best-practices/ v/1.0.0/EC 2.2	Sicherheitskontrolle/ 2.2 EC2
aws-foundational-security-best-practices/ v/1.0.0/EC 2,20	Sicherheitskontrolle/ 2.0 EC2
aws-foundational-security-best-practices/ v/1.0.0/EC 2,21	Sicherheitskontrolle/ 2.1 EC2
aws-foundational-security-best-practices/ v/1.0.0/EC 2,23	Sicherheitskontrolle/ 2.3 EC2
aws-foundational-security-best-practices/ v/1.0.0/EC 2,24	Sicherheitskontrolle/ 2.4 EC2

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-foundational-security-best-practices/ v/1.0.0/EC 2,25	Sicherheitskontrolle/ 2.5 EC2
aws-foundational-security-best-practices/ v/1.0.0/ECR 1.	Sicherheitskontrolle/ECR.1
aws-foundational-security-best- 2. practices/ v/1.0.0/ECR	Sicherheitskontrolle/ECR.2
aws-foundational-security-best- 3. practices/ v/1.0.0/ECR	Sicherheitskontrolle/ECR.3
aws-foundational-security-best- 1. practices/ v/1.0.0/ECS	Sicherheitskontrolle/ECS.1
aws-foundational-security-best- 1.0 practices/ v/1.0.0/ECS	Sicherheitskontrolle/ECS.10
aws-foundational-security-best- 1.2 practices/ v/1.0.0/ECS	Sicherheitskontrolle/ECS.12
aws-foundational-security-best- 2. practices/ v/1.0.0/ECS	Sicherheitskontrolle/ECS.2
aws-foundational-security-best- 3. practices/ v/1.0.0/ECS	Sicherheitskontrolle/ECS.3
aws-foundational-security-best- 4. practices/ v/1.0.0/ECS	Sicherheitskontrolle/ECS.4
aws-foundational-security-best- 5. practices/ v/1.0.0/ECS	Sicherheitskontrolle/ECS.5
aws-foundational-security-best- 8. practices/ v/1.0.0/ECS	Sicherheitskontrolle/ECS.8

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-foundational-security-best- 1. practices/ v/1.0.0/EFS	Sicherheitskontrolle/EFS.1
aws-foundational-security-best- 2. practices/ v/1.0.0/EFS	Sicherheitskontrolle/EFS.2
aws-foundational-security-best- 3. practices/ v/1.0.0/EFS	Sicherheitskontrolle/EFS.3
aws-foundational-security-best- 4. practices/ v/1.0.0/EFS	Sicherheitskontrolle/EFS.4
aws-foundational-security-best- 2. practices/ v/1.0.0/EKS	Sicherheitskontrolle/EKS.2
aws-foundational-security-best- 1. practices/ v/1.0.0/ElasticBeanstalk	Sicherheitskontrolle/ .1 ElasticBeanstalk
aws-foundational-security-best- practices/ v/1.0.0/ElasticBeanstalk 2.	Sicherheitskontrolle/ .2 ElasticBeanstalk
aws-foundational-security-best- practices/ v/1.0.0/ELBv 2.1	Sicherheitskontrolle/ELB.1
aws-foundational-security-best- 2.2 practices/ v/1.0.0/ELB	Sicherheitskontrolle/ELB.2
aws-foundational-security-best- 3. practices/ v/1.0.0/ELB	Sicherheitskontrolle/ELB.3
aws-foundational-security-best- 4. practices/ v/1.0.0/ELB	Sicherheitskontrolle/ELB.4
aws-foundational-security-best- 5. practices/ v/1.0.0/ELB	Sicherheitskontrolle/ELB.5

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-foundational-security-best- 6. practices/ v/1.0.0/ELB	Sicherheitskontrolle/ELB.6
aws-foundational-security-best- 7. practices/ v/1.0.0/ELB	Sicherheitskontrolle/ELB.7
aws-foundational-security-best- 8. practices/ v/1.0.0/ELB	Sicherheitskontrolle/ELB.8
aws-foundational-security-best- 9. practices/ v/1.0.0/ELB	Sicherheitskontrolle/ELB.9
aws-foundational-security-best- 1.0 practices/ v/1.0.0/ELB	Sicherheitskontrolle/ELB.10
aws-foundational-security-best- 1.1 practices/ v/1.0.0/ELB	Sicherheitskontrolle/ELB.11
aws-foundational-security-best- 1.2 practices/ v/1.0.0/ELB	Sicherheitskontrolle/ELB.12
aws-foundational-security-best- 1.3 practices/ v/1.0.0/ELB	Sicherheitskontrolle/ELB.13
aws-foundational-security-best- 1.4 practices/ v/1.0.0/ELB	Sicherheitskontrolle/ELB.14
aws-foundational-security-best- 1. practices/ v/1.0.0/EMR	Sicherheitskontrolle/EMR.1
aws-foundational-security-best- 1. practices/ v/1.0.0/ES	Sicherheitskontrolle/ES.1
aws-foundational-security-best- 2. practices/ v/1.0.0/ES	Sicherheitskontrolle/ES.2

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-foundational-security-best- 3. practices/ v/1.0.0/ES	Sicherheitskontrolle/ES.3
aws-foundational-security-best- 4. practices/ v/1.0.0/ES	Sicherheitskontrolle/ES.4
aws-foundational-security-best- 5. practices/ v/1.0.0/ES	Sicherheitskontrolle/ES.5
aws-foundational-security-best- 6. practices/ v/1.0.0/ES	Sicherheitskontrolle/ES.6
aws-foundational-security-best- 7. practices/ v/1.0.0/ES	Sicherheitskontrolle/ES.7
aws-foundational-security-best- 8. practices/ v/1.0.0/ES	Sicherheitskontrolle/ES.8
aws-foundational-security-best- 1. practices/ v/1.0.0/GuardDuty	Sicherheitskontrolle/ .1 GuardDuty
aws-foundational-security-best- practices/ v/1.0.0/IAM 1.	Sicherheitskontrolle/IAM.1
aws-foundational-security-best- 2. practices/ v/1.0.0/IAM	Sicherheitskontrolle/IAM.2
aws-foundational-security-best- 2.1 practices/ v/1.0.0/IAM	Sicherheitskontrolle/IAM.21
aws-foundational-security-best- 3. practices/ v/1.0.0/IAM	Sicherheitskontrolle/IAM.3
aws-foundational-security-best- 4. practices/ v/1.0.0/IAM	Sicherheitskontrolle/IAM.4

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-foundational-security-best- 5. practices/ v/1.0.0/IAM	Sicherheitskontrolle/IAM.5
aws-foundational-security-best- 6. practices/ v/1.0.0/IAM	Sicherheitskontrolle/IAM.6
aws-foundational-security-best- 7. practices/ v/1.0.0/IAM	Sicherheitskontrolle/IAM.7
aws-foundational-security-best- 8. practices/ v/1.0.0/IAM	Sicherheitskontrolle/IAM.8
aws-foundational-security-best- 1. practices/ v/1.0.0/Kinesis	Sicherheitskontrolle/Kinesis.1
aws-foundational-security-best- 1. practices/ v/1.0.0/KMS	Sicherheitskontrolle/KMS.1
aws-foundational-security-best- 2. practices/ v/1.0.0/KMS	Sicherheitskontrolle/KMS.2
aws-foundational-security-best- 3. practices/ v/1.0.0/KMS	Sicherheitskontrolle/KMS.3
aws-foundational-security-best- 1. practices/ v/1.0.0/Lambda	Sicherheitskontrolle/Lambda.1
aws-foundational-security-best- 2. practices/ v/1.0.0/Lambda	Sicherheitskontrolle/Lambda.2
aws-foundational-security-best- 5. practices/ v/1.0.0/Lambda	Sicherheitskontrolle/Lambda.5
aws-foundational-security-best- 3. practices/ v/1.0.0/NetworkFirewall	Sicherheitskontrolle/ .3 NetworkFirewall

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-foundational-security-best-practices/ v/1.0.0/NetworkFirewall 4.	Sicherheitskontrolle/ .4 NetworkFirewall
aws-foundational-security-best-practices/ v/1.0.0/NetworkFirewall 5.	Sicherheitskontrolle/ .5 NetworkFirewall
aws-foundational-security-best-practices/ v/1.0.0/NetworkFirewall 6.	Sicherheitskontrolle/ .6 NetworkFirewall
aws-foundational-security-best-practices/ v/1.0.0/Opensearch 1.	Sicherheitskontrolle/OpenSearch.1
aws-foundational-security-best-practices/ v/1.0.0/Opensearch 2.	Sicherheitskontrolle/OpenSearch.2
aws-foundational-security-best-practices/ v/1.0.0/Opensearch 3.	Sicherheitskontrolle/OpenSearch.3
aws-foundational-security-best-practices/ v/1.0.0/Opensearch 4.	Sicherheitskontrolle/OpenSearch.4
aws-foundational-security-best-practices/ v/1.0.0/Opensearch 5.	Sicherheitskontrolle/OpenSearch.5
aws-foundational-security-best-practices/ v/1.0.0/Opensearch 6.	Sicherheitskontrolle/OpenSearch.6
aws-foundational-security-best-practices/ v/1.0.0/Opensearch 7.	Sicherheitskontrolle/OpenSearch.7
aws-foundational-security-best-practices/ v/1.0.0/Opensearch 8.	Sicherheitskontrolle/OpenSearch.8
aws-foundational-security-best-practices/ v/1.0.0/RDS	Sicherheitskontrolle/RDS.1

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-foundational-security-best- 1.0 practices/ v/1.0.0/RDS	Sicherheitskontrolle/RDS.10
aws-foundational-security-best- 1.1 practices/ v/1.0.0/RDS	Sicherheitskontrolle/RDS.11
aws-foundational-security-best- 1.2 practices/ v/1.0.0/RDS	Sicherheitskontrolle/RDS.12
aws-foundational-security-best- 1.3 practices/ v/1.0.0/RDS	Sicherheitskontrolle/RDS.13
aws-foundational-security-best- 1.4 practices/ v/1.0.0/RDS	Sicherheitskontrolle/RDS.14
aws-foundational-security-best- 1.5 practices/ v/1.0.0/RDS	Sicherheitskontrolle/RDS.15
aws-foundational-security-best- 1.6 practices/ v/1.0.0/RDS	Sicherheitskontrolle/RDS.16
aws-foundational-security-best- 1.7 practices/ v/1.0.0/RDS	Sicherheitskontrolle/RDS.17
aws-foundational-security-best- 1.9 practices/ v/1.0.0/RDS	Sicherheitskontrolle/RDS.19
aws-foundational-security-best- 2. practices/ v/1.0.0/RDS	Sicherheitskontrolle/RDS.2
aws-foundational-security-best- 2.0 practices/ v/1.0.0/RDS	Sicherheitskontrolle/RDS.20
aws-foundational-security-best- 2.1 practices/ v/1.0.0/RDS	Sicherheitskontrolle/RDS.21

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-foundational-security-best- 2.2 practices/ v/1.0.0/RDS	Sicherheitskontrolle/RDS.22
aws-foundational-security-best- 2.3 practices/ v/1.0.0/RDS	Sicherheitskontrolle/RDS.23
aws-foundational-security-best- 2.4 practices/ v/1.0.0/RDS	Sicherheitskontrolle/RDS.24
aws-foundational-security-best- 2.5 practices/ v/1.0.0/RDS	Sicherheitskontrolle/RDS.25
aws-foundational-security-best- 3. practices/ v/1.0.0/RDS	Sicherheitskontrolle/RDS.3
aws-foundational-security-best- 4. practices/ v/1.0.0/RDS	Sicherheitskontrolle/RDS.4
aws-foundational-security-best- 5. practices/ v/1.0.0/RDS	Sicherheitskontrolle/RDS.5
aws-foundational-security-best- 6. practices/ v/1.0.0/RDS	Sicherheitskontrolle/RDS.6
aws-foundational-security-best- 7. practices/ v/1.0.0/RDS	Sicherheitskontrolle/RDS.7
aws-foundational-security-best- 8. practices/ v/1.0.0/RDS	Sicherheitskontrolle/RDS.8
aws-foundational-security-best- 9. practices/ v/1.0.0/RDS	Sicherheitskontrolle/RDS.9
aws-foundational-security-best- 1. practices/ v/1.0.0/Redshift	Sicherheitskontrolle/RedShift.1

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-foundational-security-best- 2. practices/ v/1.0.0/Redshift	Sicherheitssteuerung/RedShift.2
aws-foundational-security-best- 3. practices/ v/1.0.0/Redshift	Sicherheitskontrolle/RedShift.3
aws-foundational-security-best- 4. practices/ v/1.0.0/Redshift	Sicherheitssteuerung/RedShift.4
aws-foundational-security-best- 6. practices/ v/1.0.0/Redshift	Sicherheitssteuerung/RedShift.6
aws-foundational-security-best- 7. practices/ v/1.0.0/Redshift	Sicherheitssteuerung/RedShift.7
aws-foundational-security-best- 8. practices/ v/1.0.0/Redshift	Sicherheitssteuerung/RedShift.8
aws-foundational-security-best- 9. practices/ v/1.0.0/Redshift	Sicherheitssteuerung/RedShift.9
aws-foundational-security-best- 3.1 practices/ v/1.0.0/S	Sicherheitskontrolle/S3.1
aws-foundational-security-best- 3.12 practices/ v/1.0.0/S	Sicherheitskontrolle/S3.12
aws-foundational-security-best- 3.13 practices/ v/1.0.0/S	Sicherheitskontrolle/S3.13
aws-foundational-security-best- 3.2 practices/ v/1.0.0/S	Sicherheitskontrolle/S3.2
aws-foundational-security-best- 3.3 practices/ v/1.0.0/S	Sicherheitskontrolle/S3.3

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-foundational-security-best- 3.5 practices/ v/1.0.0/S	Sicherheitskontrolle/S3.5
aws-foundational-security-best- 3.6 practices/ v/1.0.0/S	Sicherheitskontrolle/S3.6
aws-foundational-security-best- 3.8 practices/ v/1.0.0/S	Sicherheitskontrolle/S3.8
aws-foundational-security-best- 3.9 practices/ v/1.0.0/S	Sicherheitskontrolle/3.9
aws-foundational-security-best- 1. practices/ v/1.0.0/SageMaker	Sicherheitskontrolle/ .1 SageMaker
aws-foundational-security-best- practices/ v/1.0.0/SageMaker 2.	Sicherheitskontrolle/ .2 SageMaker
aws-foundational-security-best- practices/ v/1.0.0/SageMaker 3.	Sicherheitskontrolle/ .3 SageMaker
aws-foundational-security-best- practices/ v/1.0.0/SecretsManager 1.	Sicherheitskontrolle/ .1 SecretsManager
aws-foundational-security-best- practices/ v/1.0.0/SecretsManager 2.	Sicherheitskontrolle/ .2 SecretsManager
aws-foundational-security-best- practices/ v/1.0.0/SecretsManager 3.	Sicherheitskontrolle/ .3 SecretsManager
aws-foundational-security-best- practices/ v/1.0.0/SecretsManager 4.	Sicherheitskontrolle/ .4SecretsManager.
aws-foundational-security-best- practices/ v/1.0.0/SQS 1.	Sicherheitskontrolle/SQS.1

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
aws-foundational-security-best- 1. practices/ v/1.0.0/SSM	Sicherheitskontrolle/SSM.1
aws-foundational-security-best- 1.2 practices/ v/1.0.0/SSM	Sicherheitskontrolle/SSM.2
aws-foundational-security-best- 3. practices/ v/1.0.0/SSM	Sicherheitskontrolle/SSM.3
aws-foundational-security-best- 4. practices/ v/1.0.0/SSM	Sicherheitskontrolle/SSM.4
aws-foundational-security-best- 1. practices/ v/1.0.0/WAF	Sicherheitskontrolle/WAF.1
aws-foundational-security-best- 2. practices/ v/1.0.0/WAF	Sicherheitskontrolle/WAF.2
aws-foundational-security-best- 3. practices/ v/1.0.0/WAF	Sicherheitskontrolle/WAF.3
aws-foundational-security-best- 4. practices/ v/1.0.0/WAF	Sicherheitskontrolle/WAF.4
aws-foundational-security-best- 6. practices/ v/1.0.0/WAF	Sicherheitskontrolle/WAF.6
aws-foundational-security-best- 7. practices/ v/1.0.0/WAF	Sicherheitskontrolle/WAF.7
aws-foundational-security-best- 8. practices/ v/1.0.0/WAF	Sicherheitskontrolle/WAF.8
aws-foundational-security-best- 1.0 practices/ v/1.0.0/WAF	Sicherheitskontrolle/WAF.10
pci-. dss/v/3.2.1/PCI AutoScaling1.	Sicherheitskontrolle/ .1 AutoScaling

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
pci-. dss/v/3.2.1/PCI CloudTrail1.	Sicherheitskontrolle/ .2 CloudTrail
pci-. dss/v/3.2.1/PCI CloudTrail2.	Sicherheitskontrolle/ .3 CloudTrail
pci-. dss/v/3.2.1/PCI CloudTrail3.	Sicherheitskontrolle/ .4 CloudTrail
pci-. dss/v/3.2.1/PCI CloudTrail4.	Sicherheitskontrolle/ .5 CloudTrail
pci-. dss/v/3.2.1/PCI CodeBuild1.	Sicherheitskontrolle/ .1 CodeBuild
pci-. dss/v/3.2.1/PCI CodeBuild2.	Sicherheitskontrolle/ .2 CodeBuild
pci- dss/v/3.2.1/PCI .Config.1	Sicherheitskontrolle/Config.1
pci- CW.1 dss/v/3.2.1/PCI	Sicherheitskontrolle/ 1. CloudWatch
pci-D.MS.1 dss/v/3.2.1/PCI	Sicherheitskontrolle/DMS.1
pci-. dss/v/3.2.1/PCI EC21.	Sicherheitskontrolle/ .1 EC2
pci-. dss/v/3.2.1/PCI EC22.	Sicherheitskontrolle/ .2 EC2
pci-. dss/v/3.2.1/PCI EC24.	Sicherheitskontrolle/ .12 EC2
pci-. dss/v/3.2.1/PCI EC25.	Sicherheitskontrolle/ 1.3 EC2
pci-. dss/v/3.2.1/PCI EC26.	Sicherheitskontrolle/ .6 EC2
pci-. dss/v/3.2.1/PCI ELBv21.	Sicherheitskontrolle/ELB.1
pci-.ES.1 dss/v/3.2.1/PCI	Sicherheitskontrolle/ES.2
pci-.ES.2 dss/v/3.2.1/PCI	Sicherheitskontrolle/ES.1
pci-. dss/v/3.2.1/PCI GuardDuty1.	Sicherheitskontrolle/ .1 GuardDuty
pci-I.AM.1 dss/v/3.2.1/PCI	Sicherheitskontrolle/IAM.4
pci-.IAM.2 dss/v/3.2.1/PCI	Sicherheitskontrolle/IAM.2

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
pci-.IAM.3 dss/v/3.2.1/PCI	Sicherheitskontrolle/IAM.1
pci-.IAM.4 dss/v/3.2.1/PCI	Sicherheitskontrolle/IAM.6
pci-.IAM.5 dss/v/3.2.1/PCI	Sicherheitskontrolle/IAM.9
pci-.IAM.6 dss/v/3.2.1/PCI	Sicherheitskontrolle/IAM.19
pci-.IAM.7 dss/v/3.2.1/PCI	Sicherheitskontrolle/IAM.8
pci-.IAM.8 dss/v/3.2.1/PCI	Sicherheitskontrolle/IAM.10
pci- M.S.1 dss/v/3.2.1/PCI	Sicherheitskontrolle/KMS.4
dss/v/3.2.1/PCIpci-.Lambda.1	Sicherheitskontrolle/Lambda.1
pci-. dss/v/3.2.1/PCI Lambda.2	Sicherheitskontrolle/Lambda.3
pci-. Suche öffnen.1 dss/v/3.2.1/PCI	Sicherheitskontrolle/OpenSearch.2
pci-. Opensearch.2 dss/v/3.2.1/PCI	Sicherheitskontrolle/OpenSearch.1
pci- .RDS.1 dss/v/3.2.1/PCI	Sicherheitskontrolle/RDS.1
pci-.RDS.2 dss/v/3.2.1/PCI	Sicherheitskontrolle/RDS.2
pci-. dss/v/3.2.1/PCI Redshift.1	Sicherheitskontrolle/RedShift.1
pci-S 3.1 dss/v/3.2.1/PCI	Sicherheitskontrolle/S3.3
pci-S 3.2 dss/v/3.2.1/PCI	Sicherheitskontrolle/S3.2
pci-S 3.3 dss/v/3.2.1/PCI	Sicherheitskontrolle/S3.7
pci-S 3.5 dss/v/3.2.1/PCI	Sicherheitskontrolle/S3.5
pci-S 3.6 dss/v/3.2.1/PCI	Sicherheitskontrolle/S3.1
pci-. dss/v/3.2.1/PCI SageMaker1.	Sicherheitskontrolle/ .1 SageMaker

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
pci-S.SM.1 dss/v/3.2.1/PCI	Sicherheitskontrolle/SSM.2
pci-SSM.2 dss/v/3.2.1/PCI	Sicherheitskontrolle/SSM.3
pci-.SSM.3 dss/v/3.2.1/PCI	Sicherheitskontrolle/SSM.1
service-managed-aws-control- 1. tower/v/1.0.0/ ACM	Sicherheitskontrolle/ACM.1
service-managed-aws-control- 1. tower/v/1.0.0/ APIGateway	Sicherheitskontrolle/ .1 APIGateway
service-managed-aws-control- tower/v/1.0.0/ APIGateway 2.	Sicherheitskontrolle/ .2 APIGateway
service-managed-aws-control- tower/v/1.0.0/ APIGateway 3.	Sicherheitskontrolle/ .3 APIGateway
service-managed-aws-control- tower/v/1.0.0/ APIGateway 4.	Sicherheitskontrolle/ .4APIGateway.
service-managed-aws-control- tower/v/1.0.0/ APIGateway 5.	Sicherheitskontrolle/ .5 APIGateway
service-managed-aws-control- tower/v/1.0.0/ AutoScaling 1.	Sicherheitskontrolle/ .1 AutoScaling
service-managed-aws-control- tower/v/1.0.0/ AutoScaling 2.	Sicherheitskontrolle/ .2 AutoScaling
service-managed-aws-control- tower/v/1.0.0/ AutoScaling 3.	Sicherheitskontrolle/ .3 AutoScaling
service-managed-aws-control- tower/v/1.0.0/ AutoScaling 4.	Sicherheitskontrolle/ .4AutoScaling.

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
service-managed-aws-control- tower/v/1.0.0/ Autoscaling 5.	Sicherheitskontrolle/Autoscaling.5
service-managed-aws-control- 6. tower/v/1.0.0/ AutoScaling	Sicherheitskontrolle/ .6 AutoScaling
service-managed-aws-control- tower/v/1.0.0/ AutoScaling 9.	Sicherheitskontrolle/ .9AutoScaling.
service-managed-aws-control- tower/v/1.0.0/ CloudTrail 1.	Sicherheitskontrolle/ .1 CloudTrail
service-managed-aws-control- tower/v/1.0.0/ CloudTrail 2.	Sicherheitskontrolle/ .2 CloudTrail
service-managed-aws-control- tower/v/1.0.0/ CloudTrail 4.	Sicherheitskontrolle/ .4CloudTrail.
service-managed-aws-control- tower/v/1.0.0/ CloudTrail 5.	Sicherheitskontrolle/ .5 CloudTrail
service-managed-aws-control- tower/v/1.0.0/ CodeBuild 1.	Sicherheitskontrolle/ .1 CodeBuild
service-managed-aws-control- tower/v/1.0.0/ CodeBuild 2.	Sicherheitskontrolle/ .2 CodeBuild
service-managed-aws-control- tower/v/1.0.0/ CodeBuild 4.	Sicherheitskontrolle/ .4CodeBuild.
service-managed-aws-control- tower/v/1.0.0/ CodeBuild 5.	Sicherheitskontrolle/ .5 CodeBuild
service-managed-aws-control- tower/v/1.0.0/ DMS 1.	Sicherheitskontrolle/DMS.1

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
service-managed-aws-control- 1. tower/v/1.0.0/ DynamoDB	Sicherheitskontrolle/DynamoDB.1
service-managed-aws-control- 1.2 tower/v/1 .0.0/DynamoDB	Sicherheitskontrolle/DynamoDB.2
service-managed-aws-control- 2.1 tower/v/1 .0.0/EC	Sicherheitskontrolle/ 1. EC2
service-managed-aws-control- tower/v/1.0.0/EC 2.2	Sicherheitskontrolle/ 2.2 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2,3	Sicherheitskontrolle/ 2.3 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2,4	Sicherheitskontrolle/ 4. EC2
service-managed-aws-control- tower/v/1.0.0/EC 2.6	Sicherheitskontrolle/ .6 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2,7	Sicherheitskontrolle/ 7. EC2
service-managed-aws-control- tower/v/1.0.0/EC 2,8	Sicherheitskontrolle/ 8. EC2
service-managed-aws-control- tower/v/1.0.0/EC 2,9	Sicherheitskontrolle/ 9. EC2
service-managed-aws-control- tower/v/1.0.0/EC 2,10	Sicherheitskontrolle/ 1.0 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2,15	Sicherheitskontrolle/ 1.5 EC2

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
service-managed-aws-control- tower/v/1.0.0/EC 2,16	Sicherheitskontrolle/ 1.6 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2,17	Sicherheitskontrolle/ 1.7 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2,18	Sicherheitskontrolle/ 1.8 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2,19	Sicherheitskontrolle/ 1.9 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2,20	Sicherheitskontrolle/ 2.0 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2,21	Sicherheitskontrolle/ 2.1 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2,22	Sicherheitskontrolle/ 2.2 EC2
service-managed-aws-control- tower/v/1.0.0/ ECR 1.	Sicherheitskontrolle/ECR.1
service-managed-aws-control- 2. tower/v/1.0.0/ ECR	Sicherheitskontrolle/ECR.2
service-managed-aws-control- 3. tower/v/1.0.0/ ECR	Sicherheitskontrolle/ECR.3
service-managed-aws-control- 1. tower/v/1.0.0/ ECS	Sicherheitskontrolle/ECS.1
service-managed-aws-control- 2. tower/v/1.0.0/ ECS	Sicherheitskontrolle/ECS.2

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
service-managed-aws-control- 3. tower/v/1.0.0/ ECS	Sicherheitskontrolle/ECS.3
service-managed-aws-control- 4. tower/v/1.0.0/ ECS	Sicherheitskontrolle/ECS.4
service-managed-aws-control- 5. tower/v/1.0.0/ ECS	Sicherheitskontrolle/ECS.5
service-managed-aws-control- 8. tower/v/1.0.0/ ECS	Sicherheitskontrolle/ECS.8
service-managed-aws-control- 1.0 tower/v/1 .0.0/ECS	Sicherheitskontrolle/ECS.10
service-managed-aws-control- 1.2 tower/v/1 .0.0/ECS	Sicherheitskontrolle/ECS.12
service-managed-aws-control- 1. tower/v/1.0.0/ EFS	Sicherheitskontrolle/EFS.1
service-managed-aws-control- 2. tower/v/1.0.0/ EFS	Sicherheitskontrolle/EFS.2
service-managed-aws-control- 3. tower/v/1.0.0/ EFS	Sicherheitskontrolle/EFS.3
service-managed-aws-control- 4. tower/v/1.0.0/ EFS	Sicherheitskontrolle/EFS.4
service-managed-aws-control- 2. tower/v/1.0.0/ EKS	Sicherheitskontrolle/EKS.2
service-managed-aws-control- 2. tower/v/1.0.0/ ELB	Sicherheitskontrolle/ELB.2

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
service-managed-aws-control- 3. tower/v/1.0.0/ ELB	Sicherheitskontrolle/ELB.3
service-managed-aws-control- 4. tower/v/1.0.0/ ELB	Sicherheitskontrolle/ELB.4
service-managed-aws-control- 5. tower/v/1.0.0/ ELB	Sicherheitskontrolle/ELB.5
service-managed-aws-control- 6. tower/v/1.0.0/ ELB	Sicherheitskontrolle/ELB.6
service-managed-aws-control- 7. tower/v/1.0.0/ ELB	Sicherheitskontrolle/ELB.7
service-managed-aws-control- 8. tower/v/1.0.0/ ELB	Sicherheitskontrolle/ELB.8
service-managed-aws-control- 9. tower/v/1.0.0/ ELB	Sicherheitskontrolle/ELB.9
service-managed-aws-control- 1.0 tower/v/1 .0.0/ELB	Sicherheitskontrolle/ELB.10
service-managed-aws-control- 1.2 tower/v/1 .0.0/ELB	Sicherheitskontrolle/ELB.12
service-managed-aws-control- 1.3 tower/v/1 .0.0/ELB	Sicherheitskontrolle/ELB.13
service-managed-aws-control- 1.4 tower/v/1 .0.0/ELB	Sicherheitskontrolle/ELB.14
service-managed-aws-control- 2.1 tower/v/1 .0.0/ELBv	Sicherheitskontrolle/ 1. ELBv2

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
service-managed-aws-control- tower/v/1.0.0/ EMR 1.	Sicherheitskontrolle/EMR.1
service-managed-aws-control- 1. tower/v/1.0.0/ ES	Sicherheitskontrolle/ES.1
service-managed-aws-control- 2. tower/v/1.0.0/ ES	Sicherheitskontrolle/ES.2
service-managed-aws-control- 3. tower/v/1.0.0/ ES	Sicherheitskontrolle/ES.3
service-managed-aws-control- 4. tower/v/1.0.0/ ES	Sicherheitskontrolle/ES.4
service-managed-aws-control- 5. tower/v/1.0.0/ ES	Sicherheitskontrolle/ES.5
service-managed-aws-control- 6. tower/v/1.0.0/ ES	Sicherheitskontrolle/ES.6
service-managed-aws-control- 7. tower/v/1.0.0/ ES	Sicherheitskontrolle/ES.7
service-managed-aws-control- 8. tower/v/1.0.0/ ES	Sicherheitskontrolle/ES.8
service-managed-aws-control- 1. tower/v/1.0.0/ ElasticBeanstalk	Sicherheitskontrolle/ .1 ElasticBeanstalk
service-managed-aws-control- tower/v/1.0.0/ ElasticBeanstalk 2.	Sicherheitskontrolle/ .2 ElasticBeanstalk
service-managed-aws-control- tower/v/1.0.0/ GuardDuty 1.	Sicherheitskontrolle/ .1 GuardDuty

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
service-managed-aws-control- tower/v/1.0.0/ IAM 1.	Sicherheitskontrolle/IAM.1
service-managed-aws-control- 2. tower/v/1.0.0/ IAM	Sicherheitskontrolle/IAM.2
service-managed-aws-control- 3. tower/v/1.0.0/ IAM	Sicherheitskontrolle/IAM.3
service-managed-aws-control- 4. tower/v/1.0.0/ IAM	Sicherheitskontrolle/IAM.4
service-managed-aws-control- 5. tower/v/1.0.0/ IAM	Sicherheitskontrolle/IAM.5
service-managed-aws-control- 6. tower/v/1.0.0/ IAM	Sicherheitskontrolle/IAM.6
service-managed-aws-control- 7. tower/v/1.0.0/ IAM	Sicherheitskontrolle/IAM.7
service-managed-aws-control- 8. tower/v/1.0.0/ IAM	Sicherheitskontrolle/IAM.8
service-managed-aws-control- 2.1 tower/v/1 .0.0/IAM	Sicherheitskontrolle/IAM.21
service-managed-aws-control- 1. tower/v/1.0.0/ Kinesis	Sicherheitskontrolle/Kinesis.1
service-managed-aws-control- 1. tower/v/1.0.0/ KMS	Sicherheitskontrolle/KMS.1
service-managed-aws-control- 2. tower/v/1.0.0/ KMS	Sicherheitskontrolle/KMS.2

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
service-managed-aws-control- 3. tower/v/1.0.0/ KMS	Sicherheitskontrolle/KMS.3
service-managed-aws-control- 1. tower/v/1.0.0/ Lambda	Sicherheitskontrolle/Lambda.1
service-managed-aws-control- 2. tower/v/1.0.0/ Lambda	Sicherheitskontrolle/Lambda.2
service-managed-aws-control- 5. tower/v/1.0.0/ Lambda	Sicherheitskontrolle/Lambda.5
service-managed-aws-control- 3. tower/v/1.0.0/ NetworkFirewall	Sicherheitskontrolle/ .3 NetworkFirewall
service-managed-aws-control- tower/v/1.0.0/ NetworkFirewall 4.	Sicherheitskontrolle/ .4NetworkFirewall.
service-managed-aws-control- tower/v/1.0.0/ NetworkFirewall 5.	Sicherheitskontrolle/ .5 NetworkFirewall
service-managed-aws-control- tower/v/1.0.0/ NetworkFirewall 6.	Sicherheitskontrolle/ .6 NetworkFirewall
service-managed-aws-control- tower/v/1.0.0/ Opensearch 1.	Sicherheitskontrolle/OpenSearch.1
service-managed-aws-control- 2. tower/v/1.0.0/ Opensearch	Sicherheitskontrolle/OpenSearch.2
service-managed-aws-control- 3. tower/v/1.0.0/ Opensearch	Sicherheitskontrolle/OpenSearch.3
service-managed-aws-control- 4. tower/v/1.0.0/ Opensearch	Sicherheitskontrolle/OpenSearch.4

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
service-managed-aws-control- 5. tower/v/1.0.0/ Opensearch	Sicherheitskontrolle/OpenSearch.5
service-managed-aws-control- 6. tower/v/1.0.0/ Opensearch	Sicherheitskontrolle/OpenSearch.6
service-managed-aws-control- 7. tower/v/1.0.0/ Opensearch	Sicherheitskontrolle/OpenSearch.7
service-managed-aws-control- 8. tower/v/1.0.0/ Opensearch	Sicherheitskontrolle/OpenSearch.8
service-managed-aws-control- 1. tower/v/1.0.0/ RDS	Sicherheitskontrolle/RDS.1
service-managed-aws-control- 2. tower/v/1.0.0/ RDS	Sicherheitskontrolle/RDS.2
service-managed-aws-control- 3. tower/v/1.0.0/ RDS	Sicherheitskontrolle/RDS.3
service-managed-aws-control- 4. tower/v/1.0.0/ RDS	Sicherheitskontrolle/RDS.4
service-managed-aws-control- 5. tower/v/1.0.0/ RDS	Sicherheitskontrolle/RDS.5
service-managed-aws-control- 6. tower/v/1.0.0/ RDS	Sicherheitskontrolle/RDS.6
service-managed-aws-control- 8. tower/v/1.0.0/ RDS	Sicherheitskontrolle/RDS.8
service-managed-aws-control- 9. tower/v/1.0.0/ RDS	Sicherheitskontrolle/RDS.9

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
service-managed-aws-control- 1.0 tower/v/1 .0.0/RDS	Sicherheitskontrolle/RDS.10
service-managed-aws-control- 1.1 tower/v/1 .0.0/RDS	Sicherheitskontrolle/RDS.11
service-managed-aws-control- 1.3 tower/v/1 .0.0/RDS	Sicherheitskontrolle/RDS.13
service-managed-aws-control- 1.7 tower/v/1 .0.0/RDS	Sicherheitskontrolle/RDS.17
service-managed-aws-control- 1.8 tower/v/1 .0.0/RDS	Sicherheitskontrolle/RDS.18
service-managed-aws-control- 1.9 tower/v/1 .0.0/RDS	Sicherheitskontrolle/RDS.19
service-managed-aws-control- 2.0 tower/v/1 .0.0/RDS	Sicherheitskontrolle/RDS.20
service-managed-aws-control- 2.1 tower/v/1 .0.0/RDS	Sicherheitskontrolle/RDS.21
service-managed-aws-control- 2.2 tower/v/1 .0.0/RDS	Sicherheitskontrolle/RDS.22
service-managed-aws-control- 2.3 tower/v/1 .0.0/RDS	Sicherheitskontrolle/RDS.23
service-managed-aws-control- 2.5 tower/v/1 .0.0/RDS	Sicherheitskontrolle/RDS.25
service-managed-aws-control- 1. tower/v/1.0.0/ Redshift	Sicherheitskontrolle/RedShift.1

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
service-managed-aws-control- 2. tower/v/1.0.0/ Redshift	Sicherheitssteuerung/RedShift.2
service-managed-aws-control- 4. tower/v/1.0.0/ Redshift	Sicherheitssteuerung/RedShift.4
service-managed-aws-control- 6. tower/v/1.0.0/ Redshift	Sicherheitssteuerung/RedShift.6
service-managed-aws-control- 7. tower/v/1.0.0/ Redshift	Sicherheitssteuerung/RedShift.7
service-managed-aws-control- 8. tower/v/1.0.0/ Redshift	Sicherheitssteuerung/RedShift.8
service-managed-aws-control- 9. tower/v/1.0.0/ Redshift	Sicherheitssteuerung/RedShift.9
service-managed-aws-control- 3.1 tower/v/1 .0.0/S	Sicherheitskontrolle/S3.1
service-managed-aws-control- 3.2 tower/v/1 .0.0/S	Sicherheitskontrolle/S3.2
service-managed-aws-control- 3.3 tower/v/1 .0.0/S	Sicherheitskontrolle/S3.3
service-managed-aws-control- 3.5 tower/v/1 .0.0/S	Sicherheitskontrolle/S3.5
service-managed-aws-control- 3.6 tower/v/1 .0.0/S	Sicherheitskontrolle/S3.6
service-managed-aws-control- 3.8 tower/v/1 .0.0/S	Sicherheitskontrolle/S3.8

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
service-managed-aws-control- 3.9 tower/v/1 .0.0/S	Sicherheitskontrolle/3.9
service-managed-aws-control- 3.12 tower/v/1 .0.0/S	Sicherheitskontrolle/S3.12
service-managed-aws-control- 3.13 tower/v/1 .0.0/S	Sicherheitskontrolle/S3.13
service-managed-aws-control- 1. tower/v/1.0.0/ SageMaker	Sicherheitskontrolle/ .1 SageMaker
service-managed-aws-control- tower/v/1.0.0/ SecretsManager 1.	Sicherheitskontrolle/ .1 SecretsManager
service-managed-aws-control- tower/v/1.0.0/ SecretsManager 2.	Sicherheitskontrolle/ .2 SecretsManager
service-managed-aws-control- tower/v/1.0.0/ SecretsManager 3.	Sicherheitskontrolle/ .3 SecretsManager
service-managed-aws-control- tower/v/1.0.0/ SecretsManager 4.	Sicherheitskontrolle/ .4SecretsManager.
service-managed-aws-control- tower/v/1.0.0/ SQS 1.	Sicherheitskontrolle/SQS.1
service-managed-aws-control- 1. tower/v/1.0.0/ SSM	Sicherheitskontrolle/SSM.1
service-managed-aws-control- 1.2 tower/v/1 .0.0/SSM	Sicherheitskontrolle/SSM.2
service-managed-aws-control- 3. tower/v/1.0.0/ SSM	Sicherheitskontrolle/SSM.3

GeneratorID vor der Aktivierung konsolidierter Kontrollergebnisse	GeneratorID nach der Aktivierung konsolidierter Kontrollergebnisse
service-managed-aws-control- 4. tower/v/1.0.0/SSM	Sicherheitskontrolle/SSM.4
service-managed-aws-control- 2. tower/v/1.0.0/WAF	Sicherheitskontrolle/WAF.2
service-managed-aws-control- 3. tower/v/1.0.0/WAF	Sicherheitskontrolle/WAF.3
service-managed-aws-control- 4. tower/v/1.0.0/WAF	Sicherheitskontrolle/WAF.4

Wie sich die Konsolidierung auf Kontrolle und Titel auswirkt IDs

Die Ansicht konsolidierter Kontrollen und die konsolidierten Kontrollergebnisse vereinheitlichen die Kontrolle IDs und die Titel für alle Standards. Die Begriffe Security Control ID und Security Control Title beziehen sich auf diese standardunabhängigen Werte.

Die Security Hub CSPM-Konsole zeigt standardunabhängige Titel für Sicherheitskontrolle IDs und Sicherheitskontrolle an, unabhängig davon, ob die konsolidierten Kontrollergebnisse für Ihr Konto aktiviert oder deaktiviert sind. Die CSPM-Ergebnisse von Security Hub enthalten jedoch standardspezifische Kontrolltitel für PCI DSS und CIS v1.2.0, falls konsolidierte Kontrollergebnisse für Ihr Konto deaktiviert sind. Darüber hinaus enthalten die Ergebnisse des Security Hub CSPM die standardspezifische Kontroll-ID und die Sicherheitskontroll-ID. Beispiele dafür, wie sich die Konsolidierung auf die Kontrollergebnisse auswirkt, finden Sie unter. [Stichproben von Kontrollbefunden](#)

Bei Kontrollen, die Teil des [AWS Control Tower Service-Managed-Standards](#) sind, wird das Präfix aus der Kontroll-ID und dem Titel in den Ergebnissen entfernt, wenn konsolidierte Kontrollergebnisse aktiviert sind.

Um eine Sicherheitskontrolle in Security Hub CSPM zu deaktivieren, müssen Sie alle Standardsteuerungen deaktivieren, die der Sicherheitskontrolle entsprechen. Die folgende Tabelle zeigt die Zuordnung von Sicherheitskontrollen IDs und Titeln zu standardspezifischen Kontrollen und Titeln. IDs IDs und Titel für Kontrollen, die zum FSBP-Standard (AWS Foundational Security

Best Practices) gehören, sind bereits standardunabhängig. Eine Zuordnung der Steuerelemente zu den Anforderungen von Center for Internet Security (CIS) v3.0.0 finden Sie unter [Zuordnung der Kontrollen zu den CIS-Anforderungen in jeder Version](#). Um Ihre eigenen Skripts für diese Tabelle auszuführen, können Sie [sie als CSV-Datei herunterladen](#).

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.2.0	1.1 Vermeiden Sie die Verwendung des Root-Benutzers	[CloudWatch.1] Für den Benutzer „root“ sollten ein Filter und ein Alarm für die Log-Metrik vorhanden sein
CIS v1.2.0	1.10 Stellen Sie sicher, dass die IAM-Kennwortrichtlinie die Wiederverwendung von Passwörtern	[IAM.16] Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert
CIS v1.2.0	1.11 Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft	[IAM.17] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft
CIS v1.2.0	1.12 Stellen Sie sicher, dass kein Root-Benutzerzugriffsschlüssel vorhanden ist	[IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren
CIS v1.2.0	1.13 Stellen Sie sicher, dass MFA für den Root-Benutzer aktiviert ist	[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein
CIS v1.2.0	1.14 Stellen Sie sicher, dass Hardware-MFA für den Root-Benutzer aktiviert ist	[IAM.6] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.
CIS v1.2.0	1.16 Stellen Sie sicher, dass IAM-Richtlinien nur Gruppen oder Rollen zugeordnet sind	[IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein
CIS v1.2.0	1.2 Stellen Sie sicher, dass die Multi-Faktor-Authentifizierung (MFA) für	[IAM.5] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
	alle IAM-Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen	
CIS v1.2.0	1.20 Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde mit Support	[IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS - Support
CIS v1.2.0	1.22 Stellen Sie sicher, dass keine IAM-Richtlinien erstellt werden, die volle „*: *“-Administratorrechte zulassen	[IAM.1] IAM-Richtlinien sollten keine vollen „*: *“-Administratorrechte zulassen
CIS v1.2.0	1.3 Stellen Sie sicher, dass Anmeldeinformationen, die 90 Tage oder länger nicht verwendet wurden, deaktiviert sind	[IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden
CIS v1.2.0	1.4 Stellen Sie sicher, dass die Zugangsschlüssel alle 90 Tage oder weniger gewechselt werden	[IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden
CIS v1.2.0	1.5 Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert	[IAM.11] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert
CIS v1.2.0	1.6 Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert	[IAM.12] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert
CIS v1.2.0	1.7 Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens ein Symbol erfordert	[IAM.13] Stellen Sie sicher, dass für die IAM-Passwortrichtlinie mindestens ein Symbol erforderlich ist
CIS v1.2.0	1.8 Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert	[IAM.14] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.2.0	1.9 Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert	[IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert
CIS v1.2.0	2.1 Stellen Sie sicher, dass CloudTrail es in allen Regionen aktiviert ist	[CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst
CIS v1.2.0	2.2 Stellen Sie sicher, dass die Überprüfung der Protokolldatei aktiviert ist	[CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein
CIS v1.2.0	2.3 Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist	[CloudTrail.6] Sicherstellen, dass der S3-Bucket, in dem CloudTrail Protokolle gespeichert werden, nicht öffentlich zugänglich ist
CIS v1.2.0	2.4 Stellen Sie sicher, dass die CloudTrail Pfade in CloudWatch Logs integriert sind	[CloudTrail.5] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden
CIS v1.2.0	2.5 Stellen Sie sicher, dass AWS Config es aktiviert ist	[Config.1] AWS Config sollte aktiviert sein und die serviceverknüpfte Rolle für die Ressourcenaufzeichnung verwenden
CIS v1.2.0	2.6 Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist	[CloudTrail.7] Sicherstellen, dass die S3-Bucket-Zugriffsprotokollierung für den CloudTrail S3-Bucket aktiviert ist

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.2.0	2.7 Stellen Sie sicher, dass die CloudTrail Protokolle im Ruhezustand mit KMS verschlüsselt werden CMKs	[CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben
CIS v1.2.0	2.8 Stellen Sie sicher, dass die Rotation für den vom Kunden erstellten Kunden aktiviert CMKs ist	[KMS.4] Die AWS KMS Schlüssel rotation sollte aktiviert sein
CIS v1.2.0	2.9 Stellen Sie sicher, dass die VPC-Flow-Protokollierung in allen Bereichen aktiviert ist VPCs	[EC2.6] Die VPC-Flow-Protokollierung sollte in allen aktiviert sein VPCs
CIS v1.2.0	3.1 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für nicht autorisierte API-Aufrufe vorhanden sind	[CloudWatch.2] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für nicht autorisierte API-Aufrufe vorhanden sind
CIS v1.2.0	3.10 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Sicherheitsgruppen vorhanden sind	[CloudWatch.10] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Sicherheitsgruppe vorhanden sind
CIS v1.2.0	3.11 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind	[CloudWatch.11] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind
CIS v1.2.0	3.12 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Netzwerk-Gateways vorhanden sind	[CloudWatch.12] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an Network-Gateways vorhanden sind

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.2.0	3.13 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der Routentabelle vorhanden sind	[CloudWatch.13] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Routing-Tabelle vorhanden sind
CIS v1.2.0	3.14 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für VPC-Änderungen vorhanden sind	[CloudWatch.14] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für VPC-Änderungen vorhanden sind
CIS v1.2.0	3.2 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Anmeldung in der Management Console ohne MFA vorhanden sind	[CloudWatch.3] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für die Anmeldung in der Managementkonsole ohne MFA vorhanden sind
CIS v1.2.0	3.3 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Verwendung des Root-Benutzers vorhanden sind	[CloudWatch.1] Für den Benutzer „root“ sollten ein Filter und ein Alarm für die Log-Metrik vorhanden sein
CIS v1.2.0	3.4 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen der IAM-Richtlinien vorhanden sind	[CloudWatch.4] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der IAM-Richtlinie vorhanden sind
CIS v1.2.0	3.5 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für CloudTrail Konfigurationsänderungen vorhanden sind	[CloudWatch.5] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für CloudTrail -Config--Config-Änderungen vorhanden sind
CIS v1.2.0	3.6 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Management Console Authentifizierungsfehler vorhanden sind	[CloudWatch.6] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für AWS Management Console Authentifizierungsfehler vorhanden sind

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.2.0	3.7 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm vorhanden sind, um vom Kunden erstellte Dateien zu deaktivieren oder zu löschen CMKs	[CloudWatch.7] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden verwalteten Schlüsseln vorhanden sind
CIS v1.2.0	3.8 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen der S3-Bucket-Richtlinie vorhanden sind	[CloudWatch.8] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der S3-Bucket-Richtlinie vorhanden sind
CIS v1.2.0	3.9 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Config Konfigurationsänderungen vorhanden sind	[CloudWatch.9] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für AWS Config -Config--Config-Änderungen vorhanden sind
CIS v1.2.0	4.1 Stellen Sie sicher, dass keine Sicherheitsgruppen den Zugang von 0.0.0.0/0 zu Port 22 zulassen	[EC2.13] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen
CIS v1.2.0	4.2 Stellen Sie sicher, dass keine Sicherheitsgruppen den Zugriff von 0.0.0.0/0 auf Port 3389 zulassen	[EC2.14] Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 oder: :/0 auf Port 3389 zulassen
CIS v1.2.0	4.3 Stellen Sie sicher, dass die Standardsicherheitsgruppe jeder VPC den gesamten Datenverkehr einschränkt	[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen
CIS v1.4.0	1.10 Stellen Sie sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle IAM-Benutzer aktiviert ist, die über ein Konsolenpasswort verfügen	[IAM.5] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.4.0	1.14 Stellen Sie sicher, dass die Zugangsschlüssel alle 90 Tage oder weniger gewechselt werden	[IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden
CIS v1.4.0	1.16 Stellen Sie sicher, dass IAM-Richtlinien, die volle „*: *“-Administratorrechte zulassen, nicht beigefügt sind	[IAM.1] IAM-Richtlinien sollten keine vollen „*: *“-Administratorrechte zulassen
CIS v1.4.0	1.17 Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde	[IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde
CIS v1.4.0	1.4 Stellen Sie sicher, dass kein Zugriffsschlüssel für das Root-Benutzerkonto vorhanden ist	[IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren
CIS v1.4.0	1.5 Stellen Sie sicher, dass MFA für das Root-Benutzerkonto aktiviert ist	[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein
CIS v1.4.0	1.6 Stellen Sie sicher, dass Hardware-MFA für das Root-Benutzerkonto aktiviert ist	[IAM.6] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.
CIS v1.4.0	1.7 Eliminieren Sie die Verwendung des Root-Benutzers für administrative und tägliche Aufgaben	[CloudWatch.1] Für den Benutzer „root“ sollten ein Filter und ein Alarm für die Log-Metrik vorhanden sein
CIS v1.4.0	1.8 Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestlänge von 14 oder mehr erfordert	[IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert
CIS v1.4.0	1.9 Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederverwendung von	[IAM.16] Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.4.0	2.1.2 Stellen Sie sicher, dass die S3-Bucket-Richtlinie so eingestellt ist, dass HTTP-Anfragen abgelehnt werden	[S3.5] S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erfordern
CIS v1.4.0	2.1.5.1 Die Einstellung S3 Block Public Access sollte aktiviert sein	[S3.1] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein
CIS v1.4.0	2.1.5.2 Die Einstellung S3 Block Public Access sollte auf Bucket-Ebene aktiviert sein	[S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren
CIS v1.4.0	2.2.1 Stellen Sie sicher, dass die EBS-Volume-Verschlüsselung aktiviert ist	[EC2.7] Die EBS-Standardverschlüsselung sollte aktiviert sein
CIS v1.4.0	2.3.1 Stellen Sie sicher, dass die Verschlüsselung für RDS-Instances aktiviert ist	[RDS.3] Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein.
CIS v1.4.0	3.1 Stellen Sie sicher, dass CloudTrail es in allen Regionen aktiviert ist	[CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst
CIS v1.4.0	3.2 Stellen CloudTrail Sie sicher, dass die Überprüfung der Protokolldatei aktiviert ist	[CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein
CIS v1.4.0	3.4 Stellen Sie sicher, dass die CloudTrail Pfade in Logs integriert CloudWatch sind	[CloudTrail.5] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.4.0	3.5 Stellen Sie sicher, dass AWS Config es in allen Regionen aktiviert ist	[Config.1] AWS Config sollte aktiviert sein und die serviceverknüpfte Rolle für die Ressourcenaufzeichnung verwenden
CIS v1.4.0	3.6 Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist	[CloudTrail.7] Sicherstellen, dass die S3-Bucket-Zugriffsprotokollierung für den CloudTrail S3-Bucket aktiviert ist
CIS v1.4.0	3.7 Stellen Sie sicher, dass die CloudTrail Protokolle im Ruhezustand mit KMS verschlüsselt werden CMKs	[CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben
CIS v1.4.0	3.8 Stellen Sie sicher, dass die Rotation für den vom Kunden erstellten Benutzer CMKs aktiviert ist	[KMS.4] Die AWS KMS Schlüsselrotation sollte aktiviert sein
CIS v1.4.0	3.9 Stellen Sie sicher, dass die VPC-Flow-Protokollierung in allen Bereichen aktiviert ist VPCs	[EC2.6] Die VPC-Flow-Protokollierung sollte in allen aktiviert sein VPCs
CIS v1.4.0	4.4 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen der IAM-Richtlinien vorhanden sind	[CloudWatch.4] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der IAM-Richtlinie vorhanden sind
CIS v1.4.0	4.5 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für CloudTrail Konfigurationsänderungen vorhanden sind	[CloudWatch.5] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für CloudTrail -Config--Config-Änderungen vorhanden sind

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.4.0	4.6 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Management Console Authentifizierungsfehler vorhanden sind	[CloudWatch.6] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für AWS Management Console Authentifizierungsfehler vorhanden sind
CIS v1.4.0	4.7 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm vorhanden sind, um vom Kunden erstellte Dateien zu deaktivieren oder zu löschen CMKs	[CloudWatch.7] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden verwalteten Schlüsseln vorhanden sind
CIS v1.4.0	4.8 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der S3-Bucket-Richtlinie vorhanden sind	[CloudWatch.8] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der S3-Bucket-Richtlinie vorhanden sind
CIS v1.4.0	4.9 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Config Konfigurationsänderungen vorhanden sind	[CloudWatch.9] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für AWS Config -Config--Config-Änderungen vorhanden sind
CIS v1.4.0	4.10 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Sicherheitsgruppen vorhanden sind	[CloudWatch.10] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Sicherheitsgruppe vorhanden sind
CIS v1.4.0	4.11 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind	[CloudWatch.11] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.4.0	4.12 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Netzwerk-Gateways vorhanden sind	[CloudWatch.12] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an Network-Gateways vorhanden sind
CIS v1.4.0	4.13 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der Routentabelle vorhanden sind	[CloudWatch.13] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Routing-Tabelle vorhanden sind
CIS v1.4.0	4.14 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für VPC-Änderungen vorhanden sind	[CloudWatch.14] Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für VPC-Änderungen vorhanden sind
CIS v1.4.0	5.1 Stellen Sie sicher, dass das Netzwerk keinen Zugriff von 0.0.0.0/0 zu den Verwaltungspoints des Remoteservers ACLs zulässt	[EC2.21] Das Netzwerk ACLs sollte keinen Zugang von 0.0.0.0/0 zu Port 22 oder Port 3389 zulassen
CIS v1.4.0	5.3 Stellen Sie sicher, dass die Standardsicherheitsgruppe jeder VPC den gesamten Datenverkehr einschränkt	[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen
PCI DSS v3.2.1	PCI. AutoScaling.1 Auto Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten Load Balancer-Integritätsprüfungen verwenden	[AutoScaling.1] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden
PCI DSS v3.2.1	PCI. CloudTrail.1 CloudTrail Protokolle sollten im Ruhezustand verschlüsselt werden mit AWS KMS CMKs	[CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben
PCI DSS v3.2.1	PCI. CloudTrail.2 CloudTrail sollte aktiviert sein	[CloudTrail.3] Mindestens ein CloudTrail Trail sollte aktiviert sein

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
PCI DSS v3.2.1	PCI. CloudTrail.3 Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein	[CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein
PCI DSS v3.2.1	PCI. CloudTrail.4 CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden	[CloudTrail.5] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden
PCI DSS v3.2.1	PCI. CodeBuild.1 CodeBuild GitHub oder das Bitbucket-Quell-Repository URLs sollte verwenden OAuth	[CodeBuild.1] Das CodeBuild Bitbucket-Quell-Repository URLs sollte keine vertraulichen Anmeldeinformationen enthalten
PCI DSS v3.2.1	PCI. CodeBuild.2 CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten	[CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten
PCI DSS v3.2.1	AWS Config PCI.Config.1 sollte aktiviert sein	[Config.1] AWS Config sollte aktiviert sein und die serviceverknüpfte Rolle für die Ressourcenaufzeichnung verwenden
PCI DSS v3.2.1	PCI.CW.1 Es sollten ein Log-Metrikfilter und ein Alarm für die Verwendung durch den Benutzer „root“ vorhanden sein	[CloudWatch.1] Für den Benutzer „root“ sollten ein Filter und ein Alarm für die Log-Metrik vorhanden sein
PCI DSS v3.2.1	PCI.DMS.1 Database Migration Service Service-Replikationsinstanzen sollten nicht öffentlich sein	[DMS.1] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein
PCI DSS v3.2.1	PCI. EC2.1 EBS-Snapshots sollten nicht öffentlich wiederherstellbar sein	[EC2.1] Amazon EBS-Snapshots sollten nicht öffentlich wiederherstellbar sein

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
PCI DSS v3.2.1	PCI. EC2.2 Die VPC-Standardsicherheitsgruppe sollte eingehenden und ausgehenden Datenverkehr verbieten	[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen
PCI DSS v3.2.1	PCI. EC2.4 Unbenutzte EC2 EIPs sollten entfernt werden	[EC2.12] Unbenutztes Amazon EC2 EIPs sollte entfernt werden
PCI DSS v3.2.1	PCI. EC2.5 Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 zu Port 22 zulassen	[EC2.13] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen
PCI DSS v3.2.1	PCI. EC2.6 Die VPC-Flow-Protokollierung sollte in allen aktiviert sein VPCs	[EC2.6] Die VPC-Flow-Protokollierung sollte in allen aktiviert sein VPCs
PCI DSS v3.2.1	PCI. ELBv2.1 Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden	[ELB.1] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden
PCI DSS v3.2.1	PCI.ES.1 Elasticsearch-Domains sollten sich in einer VPC befinden	[ES.2] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein
PCI DSS v3.2.1	Bei PCI.ES.2 Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein	[ES.1] Bei Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
PCI DSS v3.2.1	PCI. GuardDuty.1 GuardDuty sollte aktiviert sein	[GuardDuty.1] GuardDuty sollte aktiviert sein
PCI DSS v3.2.1	PCI.IAM.1 Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren	[IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren
PCI DSS v3.2.1	PCI.IAM.2 IAM-Benutzern sollten keine IAM-Richtlinien zugewiesen sein	[IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
PCI DSS v3.2.1	PCI.IAM.3 IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen	[IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen
PCI DSS v3.2.1	PCI.IAM.4 Hardware MFA sollte für den Root-Benutzer aktiviert sein	[IAM.6] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.
PCI DSS v3.2.1	PCI.IAM.5 Virtual MFA sollte für den Root-Benutzer aktiviert sein	[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein
PCI DSS v3.2.1	PCI.IAM.6 MFA sollte für alle IAM-Benutzer aktiviert sein	[IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein
PCI DSS v3.2.1	PCI.IAM.7 IAM-Benutzeranmeldedaten sollten deaktiviert werden, wenn sie nicht innerhalb einer vordefinierten Anzahl von Tagen verwendet werden	[IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden
PCI DSS v3.2.1	PCI.IAM.8-Passwortrichtlinien für IAM-Benutzer sollten solide Konfigurationen haben	[IAM.10] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein
PCI DSS v3.2.1	PCI.KMS.1 Die CMK-Rotation (Customer Master Key) sollte aktiviert sein	[KMS.4] Die AWS KMS Schlüsselrotation sollte aktiviert sein
PCI DSS v3.2.1	PCI.Lambda.1 Lambda-Funktionen sollten den öffentlichen Zugriff verbieten	[Lambda.1] Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten
PCI DSS v3.2.1	PCI.Lambda.2 Lambda-Funktionen sollten sich in einer VPC befinden	[Lambda.3] Lambda-Funktionen sollten sich in einer VPC befinden
PCI DSS v3.2.1	OpenSearch PCI.OpenSearch.1-Domains sollten sich in einer VPC befinden	[Opensearch.2] OpenSearch - Domains sollten nicht öffentlich zugänglich sein

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
PCI DSS v3.2.1	PCI.OpenSearch.2 EBS-Snapshots sollten nicht öffentlich wiederherstellbar sein	Bei [Opensearch.1] OpenSearch - Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
PCI DSS v3.2.1	Der PCI.RDS.1 RDS-Snapshot sollte privat sein	[RDS.1] Der RDS-Snapshot sollte privat sein
PCI DSS v3.2.1	PCI.RDS.2 RDS-DB-Instances sollten den öffentlichen Zugriff verbieten	[RDS.2] RDS-DB-Instances sollten, wie in der Konfiguration festgelegt, den öffentlichen Zugriff verbieten PubliclyAccessible
PCI DSS v3.2.1	PCI.redshift.1 Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten	[Redshift.1] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten
PCI DSS v3.2.1	PCI.S3.1 S3-Buckets sollten öffentlichen Schreibzugriff verbieten	[S3.3] S3-Allzweck-Buckets sollten den öffentlichen Schreibzugriff blockieren
PCI DSS v3.2.1	PCI.S3.2 S3-Buckets sollten öffentlichen Lesezugriff verbieten	[S3.2] S3-Allzweck-Buckets sollten den öffentlichen Lesezugriff blockieren
PCI DSS v3.2.1	Bei PCI.S3.3 S3-Buckets sollte die regionsübergreifende Replikation aktiviert sein	[S3.7] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden
PCI DSS v3.2.1	PCI.S3.5 S3-Buckets sollten Anfragen zur Verwendung von Secure Socket Layer erfordern	[S3.5] S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erfordern
PCI DSS v3.2.1	Die Einstellung PCI.S3.6 S3 Block Public Access sollte aktiviert sein	[S3.1] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
PCI DSS v3.2.1	PCI. SageMaker.1 SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben	[SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben
PCI DSS v3.2.1	Von Systems Manager verwaltete EC2 PCI.SSM.1-Instanzen sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben	[SSM.2] Von Systems Manager verwaltete EC2 Amazon-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben
PCI DSS v3.2.1	Von Systems Manager verwaltete EC2 PCI.SSM.2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben	[SSM.3] Von Systems Manager verwaltete EC2 Amazon-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben
PCI DSS v3.2.1	PCI.SSM.3-Instanzen sollten verwaltet EC2 werden von AWS Systems Manager	[SSM.1] EC2 Amazon-Instances sollten verwaltet werden von AWS Systems Manager

Aktualisierung der Workflows für die Konsolidierung

Wenn Ihre Workflows nicht auf dem spezifischen Format der Felder in den Kontrollergebnissen basieren, sind keine Maßnahmen erforderlich.

Wenn Ihre Workflows auf dem spezifischen Format eines oder mehrerer Felder in Kontrollergebnissen basieren, wie in den obigen Tabellen angegeben, sollten Sie Ihre Workflows aktualisieren. Wenn Sie beispielsweise eine EventBridge Amazon-Regel erstellt haben, die eine Aktion für eine bestimmte Kontroll-ID ausgelöst hat, z. B. das Aufrufen einer AWS Lambda Funktion, wenn die Kontroll-ID CIS 2.7 entspricht, aktualisieren Sie die Regel so, dass sie CloudTrail .2 verwendet, was der Wert für das `Compliance.SecurityControlId` Feld für dieses Steuerelement ist.

Wenn Sie [benutzerdefinierte Erkenntnisse](#) erstellt haben, die Felder oder Werte verwenden, die sich geändert haben, aktualisieren Sie diese Erkenntnisse, sodass sie die neuen Felder oder Werte verwenden.

Erforderliche ASFF-Attribute der obersten Ebene

Die folgenden Attribute der obersten Ebene im AWS Security Finding Format (ASFF) sind für alle Ergebnisse in Security Hub CSPM erforderlich. Weitere Informationen zu diesen Attributen finden Sie [AwsSecurityFinding](#) in der AWS Security Hub Hub-API-Referenz.

AwsAccountId

Die AWS-Konto ID, für die das Ergebnis gilt.

Beispiel

```
"AwsAccountId": "111111111111"
```

CreatedAt

Gibt an, wann das potenzielle Sicherheitsproblem oder das Ereignis, das durch einen Befund erfasst wurde, verursacht wurde.

Beispiel

```
"CreatedAt": "2017-03-22T13:22:13.933Z"
```

Beschreibung

Die Beschreibung eines Fundes. Dieses Feld kann unspezifischen Standardtext oder spezifische Details für die Instance des Fundes enthalten.

Für Kontrollergebnisse, die Security Hub CSPM generiert, enthält dieses Feld eine Beschreibung der Kontrolle.

Dieses Feld verweist nicht auf einen Standard, wenn Sie [konsolidierte Kontrollergebnisse](#) aktivieren.

Beispiel

```
"Description": "This AWS control checks whether AWS Config is enabled in the current account and Region."
```

GeneratorId

Die Kennung für die lösungsspezifische Komponente (eine separate Logikeinheit), die einen Fund generiert hat.

Bei Kontrollergebnissen, die Security Hub CSPM generiert, verweist dieses Feld nicht auf einen Standard, wenn Sie [konsolidierte Kontrollergebnisse](#) aktivieren.

Beispiel

```
"GeneratorId": "security-control/Config.1"
```

Id

Die produktspezifische Kennung für einen Fund. Für Kontrollergebnisse, die Security Hub CSPM generiert, enthält dieses Feld den Amazon-Ressourcennamen (ARN) des Ergebnisses.

Dieses Feld verweist nicht auf einen Standard, wenn Sie [konsolidierte Kontrollergebnisse](#) aktivieren.

Beispiel

```
"Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/iam.9/finding/ab6d6a26-a156-48f0-9403-115983e5a956"
```

ProductArn

Der von Security Hub CSPM generierte Amazon-Ressourcenname (ARN), der ein Finding-Produkt eines Drittanbieters eindeutig identifiziert, nachdem das Produkt bei Security Hub CSPM registriert wurde.

Das Format des Felds ist `arn:partition:securityhub:region:account-id:product/company-id/product-id`.

- **AWS-Services** Damit sie in Security Hub CSPM integriert sind, `company-id` müssen sie "aws" lauten, und das `product-id` muss der Name des AWS öffentlichen Dienstes sein. Da AWS Produkte und Dienstleistungen keinem Konto zugeordnet sind, ist der `account-id` Bereich des ARN leer. AWS-Services die noch nicht in Security Hub CSPM integriert sind, gelten als Produkte von Drittanbietern.
- Für öffentliche Produkte müssen die `company-id` und die `product-id` die ID-Werte sein, die zum Zeitpunkt der Registrierung angegeben wurden.
- Für private Produkte muss die `company-id` die Konto-ID sein. Die `product-id` muss das reservierte Wort "default" (Standard) oder die ID sein, die zum Zeitpunkt der Registrierung angegeben wurde.

Beispiel

```
// Private ARN
  "ProductArn": "arn:aws:securityhub:us-east-1:111111111111:product/111111111111/default"

// Public ARN
  "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty"
  "ProductArn": "arn:aws:securityhub:us-west-2:222222222222:product/generico/secure-pro"
```

Ressourcen

Das Resources Array von Objekten stellt eine Reihe von Ressourcendatentypen bereit, die die AWS Ressourcen beschreiben, auf die sich das Ergebnis bezieht. Einzelheiten zu den Feldern, die ein Resources Objekt enthalten kann, einschließlich der Felder, die erforderlich sind, finden Sie [Resource](#) in der AWS Security Hub Hub-API-Referenz. Beispiele für bestimmte Resources Objekte finden Sie AWS-Services unter [ResourcesASFF-Objekt](#).

Beispiel

```
"Resources": [
  {
    "ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/SampleApp/1234567890abcdef0",
    "ApplicationName": "SampleApp",
    "DataClassification": {
      "DetailedResultsLocation": "Path_to_Folder_or_File",
      "Result": {
        "MimeType": "text/plain",
        "SizeClassified": 2966026,
        "AdditionalOccurrences": false,
        "Status": {
          "Code": "COMPLETE",
          "Reason": "Unsupportedfield"
        },
        "SensitiveData": [
          {
            "Category": "PERSONAL_INFORMATION",
            "Detections": [
              {
                "Count": 34,
```

```

        "Type": "GE_PERSONAL_ID",
        "Occurrences": {
            "LineRanges": [
                {
                    "Start": 1,
                    "End": 10,
                    "StartColumn": 20
                }
            ],
            "Pages": [],
            "Records": [],
            "Cells": []
        }
    },
    {
        "Count": 59,
        "Type": "EMAIL_ADDRESS",
        "Occurrences": {
            "Pages": [
                {
                    "PageNumber": 1,
                    "OffsetRange": {
                        "Start": 1,
                        "End": 100,
                        "StartColumn": 10
                    },
                    "LineRange": {
                        "Start": 1,
                        "End": 100,
                        "StartColumn": 10
                    }
                }
            ]
        }
    },
    {
        "Count": 2229,
        "Type": "URL",
        "Occurrences": {
            "LineRanges": [
                {
                    "Start": 1,
                    "End": 13
                }
            ]
        }
    }

```

```

        ]
      }
    },
    {
      "Count": 13826,
      "Type": "NameDetection",
      "Occurrences": {
        "Records": [
          {
            "RecordIndex": 1,
            "JsonPath": "$.ssn.value"
          }
        ]
      }
    },
    {
      "Count": 32,
      "Type": "AddressDetection"
    }
  ],
  "TotalCount": 32
}
],
"CustomDataIdentifiers": {
  "Detections": [
    {
      "Arn": "1712be25e7c7f53c731fe464f1c869b8",
      "Name": "1712be25e7c7f53c731fe464f1c869b8",
      "Count": 2
    }
  ],
  "TotalCount": 2
}
},
{
  "Type": "AwsEc2Instance",
  "Id": "arn:aws:ec2:us-west-2:123456789012:instance/i-abcdef01234567890",
  "Partition": "aws",
  "Region": "us-west-2",
  "ResourceRole": "Target",
  "Tags": {
    "billingCode": "Lotus-1-2-3",
    "needsPatching": true
  }
},

```

```

"Details": {
  "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
  "ImageId": "ami-79fd7eee",
  "IPv4Addresses": ["1.1.1.1"],
  "IPv6Addresses": ["2001:db8:1234:1a2b::123"],
  "KeyName": "testkey",
  "LaunchedAt": "2018-09-29T01:25:54Z",
  "MetadataOptions": {
    "HttpEndpoint": "enabled",
    "HttpProtocolIpv6": "enabled",
    "HttpPutResponseHopLimit": 1,
    "HttpTokens": "optional",
    "InstanceMetadataTags": "disabled"
  }
},
"NetworkInterfaces": [
  {
    "NetworkInterfaceId": "eni-e5aa89a3"
  }
],
"SubnetId": "PublicSubnet",
"Type": "i3.xlarge",
"VirtualizationType": "hvm",
"VpcId": "TestVPCIPv6"
}
]

```

SchemaVersion

Die Schemaversion, für die ein Fund formatiert ist. Der Wert dieses Feldes muss eine der offiziell veröffentlichten Versionen sein, die von AWS identifiziert wurden. In der aktuellen Version ist die Schemaversion des AWS Security Finding Formats **2018-10-08**.

Beispiel

```
"SchemaVersion": "2018-10-08"
```

Schweregrad

Definiert die Wichtigkeit eines Ergebnisses. Einzelheiten zu diesem Objekt finden Sie [Severity](#) in der AWS Security Hub Cloud Security Posture Management (CSPM) API-Referenz.

Severity ist sowohl ein Objekt der obersten Ebene in einem Befund als auch ein unter dem Objekt verschachteltes Objekt. `FindingProviderFields`

Der Wert des Severity Objekts der obersten Ebene für einen Befund sollte nur mithilfe der API aktualisiert werden. [BatchUpdateFindings](#)

Um Informationen zum Schweregrad bereitzustellen, sollten Suchanbieter `FindingProviderFields` bei einer [BatchImportFindings](#) API-Anfrage das Severity Objekt unter aktualisieren.

Wenn eine `BatchImportFindings` Anfrage für ein neues Ergebnis nur liefert `Label` oder nur liefert `Normalized`, füllt Security Hub CSPM automatisch den Wert des anderen Felds aus. Die `Original` Felder `Product` und können ebenfalls ausgefüllt werden.

Wenn das `Finding.Severity` Objekt der obersten Ebene vorhanden, aber nicht vorhanden `Finding.FindingProviderFields` ist, erstellt Security Hub CSPM das `FindingProviderFields.Severity` Objekt und kopiert das gesamte `Finding.Severity` object Objekt hinein. Dadurch wird sichergestellt, dass die ursprünglichen, vom Anbieter bereitgestellten Details in der `FindingProviderFields.Severity` Struktur beibehalten werden, auch wenn das Objekt der obersten Ebene überschrieben wird. `Severity`

Der Schweregrad des Ergebnisses berücksichtigt nicht den kritischen Charakter der beteiligten Komponenten oder der zugrunde liegenden Ressource. Der kritische Charakter ist definiert als die Wichtigkeit der Ressourcen, die mit dem Ergebnis verbunden sind. Beispielsweise hat eine Ressource, die einer geschäftskritischen Anwendung zugeordnet ist, eine höhere Priorität als eine Ressource, die nicht produktionstechnischen Tests zugeordnet ist. Verwenden Sie das `Criticality`-Feld, um Informationen zum kritischen Charakter der Ressource zu erfassen.

Wir empfehlen, bei der Übersetzung der systemeigenen Schweregrade der Ergebnisse in den Wert von im ASFF die folgenden Hinweise zu beachten. `Severity.Label`

- **INFORMATIONAL**— Diese Kategorie kann einen Befund für einen `PASSED`, `WARNING`, oder `NOT AVAILABLE` Scheck oder eine Identifizierung sensibler Daten beinhalten.
- **LOW**— Erkenntnisse, die zu future Kompromissen führen könnten. Zu dieser Kategorie können beispielsweise Sicherheitslücken, Konfigurationsschwächen und offengelegte Passwörter gehören.
- **MEDIUM**— Ergebnisse, die auf einen aktiven Kompromiss hindeuten, aber keinen Hinweis darauf, dass ein Gegner seine Ziele erreicht hat. Zu dieser Kategorie können beispielsweise Malware-Aktivitäten, Hacking-Aktivitäten und die Erkennung ungewöhnlicher Verhaltensweisen gehören.

- **HIGHoder CRITICAL** — Ergebnisse, die darauf hindeuten, dass ein Angreifer seine Ziele erreicht hat, wie z. B. aktiver Datenverlust oder Datenkompromittierung oder Denial-of-Service.

Beispiel

```
"Severity": {
  "Label": "CRITICAL",
  "Normalized": 90,
  "Original": "CRITICAL"
}
```

Title

Der Titel eines Fundes. Dieses Feld kann unspezifischen Standardtext oder spezifische Details für diese Instanz des Fundes enthalten.

Bei Kontrollergebnissen gibt dieses Feld den Titel der Kontrolle an. Dieses Feld verweist nicht auf einen Standard, wenn Sie [konsolidierte Kontrollergebnisse](#) aktivieren.

Beispiel

```
"Title": "AWS Config should be enabled"
```

Typen

Ein oder mehrere Fundtypen im Format *namespace/category/classifier*, die einen Fund klassifizieren. Dieses Feld verweist nicht auf einen Standard, wenn Sie [konsolidierte Kontrollergebnisse](#) aktivieren.

Typessollte nur mithilfe der [BatchUpdateFindings](#)API aktualisiert werden.

Wenn Sie nach Anbietern suchen, für die Sie einen Wert angeben möchten, Types sollten Sie das Types Attribut unter verwenden [FindingProviderFields](#).

In der folgenden Liste sind die Aufzählungszeichen der obersten Ebene Namespaces, die Aufzählungszeichen der zweiten Ebene Kategorien und die Aufzählungszeichen der dritten Ebene Klassifikatoren. Wir empfehlen, dass Suchanbieter definierte Namespaces verwenden, um Ergebnisse zu sortieren und zu gruppieren. Die definierten Kategorien und Klassifikatoren

können ebenfalls verwendet werden, sind aber nicht erforderlich. Nur der Software- und Konfigurationsprüfungs-Namespace hat definierte Klassifizierer.

Sie können einen Teilpfad für namespace/category/classifier definieren. Beispielsweise sind die folgenden Findetypen alle gültig:

- TTPs
- TTPs/Umgehung der Verteidigung
- TTPs/Defense Evasion/CloudTrailStopped

Die Kategorien Taktiken, Techniken und Verfahren (TTPs) in der folgenden Liste entsprechen der [MITRE ATT&CK](#) Matrix™. Der Namespace Unusual Behaviors spiegelt allgemeines ungewöhnliches Verhalten wider, wie z. B. allgemeine statistische Anomalien, und ist nicht auf ein bestimmtes TTP abgestimmt. Sie können ein Ergebnis jedoch sowohl nach ungewöhnlichem Verhalten als auch nach Befundtypen klassifizieren. TTPs

Liste der Namespaces, Kategorien und Klassifikatoren:

- Software- und Konfigurationsprüfungen
 - Schwachstellen
 - CVE
 - AWS Bewährte Methoden im Bereich Sicherheit
 - Netzwerkerreichbarkeit
 - Laufzeitverhaltens-Analyse
 - Branchen- und regulatorische Standards
 - AWS Bewährte grundlegende Sicherheitsmethoden
 - CIS-Benchmarks zur Host-Härtung
 - Maßstab für AWS GUS-Stiftungen
 - PCI-DSS
 - Cloud Security Alliance-Kontrollen
 - ISO 90001-Kontrollen
 - ISO 27001-Kontrollen
 - ISO 27017-Kontrollen
 - ISO 27018-Kontrollen

- SOC 1
 - SOC 2
 - HIPAA-Kontrollen (USA)
 - NIST 800-53-Kontrollen (USA)
 - NIST CSF-Kontrollen (USA)
 - IRAP-Kontrollen (Australien)
 - K-ISMS-Kontrollen (Korea)
 - MTCS-Kontrollen (Singapur)
 - FISC-Kontrollen (Japan)
 - My Number Act-Kontrollen (Japan)
 - ENS-Kontrollen (Spanien)
 - Cyber Essentials Plus-Kontrollen (Vereinigtes Königreich)
 - G-Cloud-Kontrollen (Vereinigtes Königreich)
 - C5-Kontrollen (Deutschland)
 - IT-Grundschutz-Kontrollen (Deutschland)
 - DSGVO-Kontrollen (Europa)
 - TISAX-Kontrollen (Europa)
 - Patch-Management
 - TTPs
 - Anfänglicher Zugriff
 - Ausführung
 - Persistenz
 - Rechteeskalation
 - Abwehrumgehung
 - Anmeldeinformationszugriff
 - Erkennung
 - Seitwärtsbewegung (Lateral Movement)
 - Sammlung
 - **Command and Control**
-
- Erforderliche ASFF-Attribute der obersten Ebene
- Auswirkungen

- Offenlegung von Daten
- Datenexfiltration
- Datenvernichtung
- Denial of Service
- Ressourcennutzung
- Ungewöhnliches Verhalten
 - Anwendung
 - Netzwerkfluss
 - IP-Adresse
 - Benutzer
 - VM
 - Container
 - Serverless
 - Prozess
 - Datenbank
 - Daten
- Identifizierung sensibler Daten
 - Personenbezogene Daten
 - Passwörter
 - Recht
 - Finanzanwendungen
 - Sicherheit
 - Geschäft

Beispiel

```
"Types": [  
  "Software and Configuration Checks/Vulnerabilities/CVE"  
]
```

UpdatedAt

Gibt an, wann der Suchprovider den Suchdatensatz zuletzt aktualisiert hat.

Dieser Zeitstempel gibt den Zeitpunkt an, zu dem der Suchdatensatz zuletzt oder zuletzt aktualisiert wurde. Folglich kann er vom LastObservedAt Zeitstempel abweichen, der angibt, wann das Ereignis oder die Sicherheitsanfälligkeit zuletzt oder zuletzt beobachtet wurde.

Wenn Sie den Funddatensatz aktualisieren, müssen Sie diesen Zeitstempel durch den aktualisierten Zeitstempel ersetzen. Bei der Erstellung eines Befunddatensatzes müssen die Zeitstempel CreatedAt und die UpdatedAt Zeitstempel identisch sein. Nach einer Aktualisierung des Suchdatensatzes muss der Wert dieses Felds aktueller sein als alle vorherigen Werte, die es enthielt.

Beachten Sie, dass dieser [BatchUpdateFindings](#) Vorgang UpdatedAt nicht aktualisiert werden kann. Sie können es nur mithilfe von [BatchImportFindings](#) Operation aktualisieren.

Beispiel

```
"UpdatedAt": "2017-04-22T13:22:13.933Z"
```

Optionale ASFF-Attribute der obersten Ebene

Die folgenden Attribute der obersten Ebene im AWS Security Finding Format (ASFF) sind für Ergebnisse in Security Hub CSPM optional. Weitere Informationen zu diesen Attributen finden Sie [AwsSecurityFinding](#) in der AWS Security Hub Hub-API-Referenz.

Aktion

Das [Action](#) Objekt enthält Details zu einer Aktion, die sich auf eine Ressource auswirkt oder auf einer Ressource ausgeführt wurde.

Beispiel

```
"Action": {
  "ActionType": "PORT_PROBE",
  "PortProbeAction": {
    "PortProbeDetails": [
      {
        "LocalPortDetails": {
          "Port": 80,
          "PortName": "HTTP"
        }
      }
    ]
  }
}
```

```

    },
    "LocalIpDetails": {
      "IpAddressV4": "192.0.2.0"
    },
    "RemoteIpDetails": {
      "Country": {
        "CountryName": "Example Country"
      },
      "City": {
        "CityName": "Example City"
      },
      "GeoLocation": {
        "Lon": 0,
        "Lat": 0
      },
      "Organization": {
        "AsnOrg": "ExampleASO",
        "Org": "ExampleOrg",
        "Isp": "ExampleISP",
        "Asn": 64496
      }
    }
  },
  "Blocked": false
}

```

AwsAccountName

Der AWS-Konto Name, auf den sich das Ergebnis bezieht.

Beispiel

```
"AwsAccountName": "jane-doe-testaccount"
```

CompanyName

Der Name des Unternehmens für das Produkt, das zu dem Ergebnis geführt hat. Bei Ergebnissen, die auf Kontrollen beruhen, lautet das Unternehmen. AWS

Security Hub CSPM füllt dieses Attribut automatisch für jeden Befund aus. Sie können es nicht mit oder aktualisieren. [BatchImportFindingsBatchUpdateFindings](#) Die Ausnahme ist, wenn

Sie eine benutzerdefinierte Integration verwenden. Siehe [the section called “Maßgeschneiderte Produktintegrationen”](#).

Wenn Sie die Security Hub CSPM-Konsole verwenden, um Ergebnisse nach Firmennamen zu filtern, verwenden Sie dieses Attribut. Wenn Sie die Security Hub CSPM-API verwenden, um Ergebnisse nach Firmennamen zu filtern, verwenden Sie das `aws/securityhub/CompanyName` Attribut unter `ProductFields`. Security Hub CSPM synchronisiert diese beiden Attribute nicht.

Beispiel

```
"CompanyName": "AWS"
```

Compliance

Das [Compliance](#) Objekt enthält in der Regel Details zu einem Kontrollergebnis, wie z. B. geltende Standards und den Status der Kontrollprüfung.

Beispiel

```
"Compliance": {
  "AssociatedStandards": [
    {"StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
    {"StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"},
    {"StandardsId": "standards/nist-800-53/v/5.0.0"}
  ],
  "RelatedRequirements": [
    "NIST.800-53.r5 AC-4",
    "NIST.800-53.r5 AC-4(21)",
    "NIST.800-53.r5 SC-7",
    "NIST.800-53.r5 SC-7(11)",
    "NIST.800-53.r5 SC-7(16)",
    "NIST.800-53.r5 SC-7(21)",
    "NIST.800-53.r5 SC-7(4)",
    "NIST.800-53.r5 SC-7(5)"
  ],
  "SecurityControlId": "EC2.18",
  "SecurityControlParameters": [
    {
      "Name": "authorizedTcpPorts",
      "Value": ["80", "443"]
    },
    {
```



```

        "Name": "authorizedUdpPorts",
        "Value": ["427"]
    },
    ],
    "Status": "NOT_AVAILABLE",
    "StatusReasons": [
        {
            "ReasonCode": "CONFIG_RETURNS_NOT_APPLICABLE",
            "Description": "This finding has a compliance status of NOT AVAILABLE because AWS Config sent Security Hub CSPM a finding with a compliance state of Not Applicable. The potential reasons for a Not Applicable finding from Config are that (1) a resource has been moved out of scope of the Config rule; (2) the Config rule has been deleted; (3) the resource has been deleted; or (4) the logic of the Config rule itself includes scenarios where Not Applicable is returned. The specific reason why Not Applicable is returned is not available in the Config rule evaluation."
        }
    ]
}

```

Wahrscheinlichkeit

Die Wahrscheinlichkeit, dass ein Ergebnis das Verhalten oder das Problem, das identifiziert werden sollte, genau identifiziert.

Confidencesollte nur mit aktualisiert werden [BatchUpdateFindings](#).

Wenn Sie nach Anbietern suchen, für die Sie einen Wert angeben möchten, Confidence sollten Sie das Confidence Attribut unter verwendenFindingProviderFields. Siehe [the section called "Aktualisierung der Ergebnisse mit FindingProviderFields"](#).

Confidencewird anhand einer Verhältnisskala auf einer Basis von 0—100 bewertet. 0 bedeutet 0 Prozent Konfidenz, und 100 bedeutet 100 Prozent Konfidenz. Beispielsweise hat eine Erkennung einer Datenexfiltration, die auf einer statistischen Abweichung des Netzwerkverkehrs basiert, eine geringe Zuverlässigkeit, da eine tatsächliche Exfiltration nicht verifiziert wurde.

Beispiel

```
"Confidence": 42
```

Kritikalität

Die Wichtigkeit, die den Ressourcen zugewiesen wird, die mit einem Ergebnis verknüpft sind.

Criticality sollte nur durch Aufrufen der [BatchUpdateFindings](#) API-Operation aktualisiert werden. Aktualisieren Sie dieses Objekt nicht mit [BatchImportFindings](#).

Wenn Sie nach Anbietern suchen, für die Sie einen Wert angeben möchten, Criticality sollten Sie das Criticality Attribut unter verwenden `FindingProviderFields`. Siehe [the section called "Aktualisierung der Ergebnisse mit FindingProviderFields"](#).

Criticality wird auf einer Basis von 0—100 bewertet, wobei eine Verhältnisskala verwendet wird, die nur ganze Zahlen unterstützt. Ein Wert von 0 bedeutet, dass die zugrunde liegenden Ressourcen keine Kritikalität haben, und der Wert 100 ist den wichtigsten Ressourcen vorbehalten.

Beachten Sie bei der Zuweisung für jede Ressource Folgendes: Criticality

- Enthält die betroffene Ressource sensible Daten (z. B. einen S3-Bucket mit PII)?
- Ermöglicht die betroffene Ressource einem Angreifer, seinen Zugriff zu vertiefen oder seine Fähigkeiten zur Ausführung zusätzlicher bösartiger Aktivitäten auszuweiten (z. B. ein kompromittiertes Systemadministratorkonto)?
- Ist die Ressource ein geschäftskritisches Asset (z. B. ein wesentliches Unternehmenssystem, dessen Kompromittierung bedeutende Umsatzeinbußen verursachen könnte)?

Sie können die folgenden Richtlinien verwenden:

- Eine Ressource, die geschäftskritische Systeme mit Strom versorgt oder hochsensible Daten enthält, kann im Bereich von 75 bis 100 bewertet werden.
- Eine Ressource, die wichtige (aber nicht kritische Systeme) mit Strom versorgt oder mäßig wichtige Daten enthält, kann im Bereich 25—74 bewertet werden.
- Eine Ressource, die unwichtige Systeme unterstützt oder unsensible Daten enthält, sollte im Bereich von 0—24 bewertet werden.

Beispiel

```
"Criticality": 99
```

Erkennung

Das Detection Objekt enthält Details zu einer Angriffssequenz, die von Amazon GuardDuty Extended Threat Detection gefunden wurde. GuardDuty generiert eine Erkennung der

Angriffssequenz, wenn mehrere Ereignisse auf eine potenziell verdächtige Aktivität zurückzuführen sind. Um Informationen zur GuardDuty Angriffssequenz in AWS Security Hub Cloud Security Posture Management (CSPM) zu erhalten, müssen Sie die GuardDuty Aktivierung in Ihrem Konto aktiviert haben. Weitere Informationen finden Sie unter [Amazon GuardDuty Extended Threat Detection](#) im GuardDuty Amazon-Benutzerhandbuch.

Beispiel

```
"Detection": {
  "Sequence": {
    "Uid": "111111111111-184ec3b9-cf8d-452d-9aad-f5bdb7afb010",
    "Actors": [{
      "Id": "USER:ARO987654321EXAMPLE:i-b188560f:1234567891",
      "Session": {
        "Uid": "1234567891",
        "MfaStatus": "DISABLED",
        "CreatedTime": "1716916944000",
        "Issuer": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
      },
      "User": {
        "CredentialUid": "ASIAIOSFODNN7EXAMPLE",
        "Name": "ec2_instance_role_production",
        "Type": "AssumedRole",
        "Uid": "ARO987654321EXAMPLE:i-b188560f",
        "Account": {
          "Uid": "AccountId",
          "Name": "AccountName"
        }
      }
    }],
    "Endpoints": [{
      "Id": "EndpointId",
      "Ip": "203.0.113.1",
      "Domain": "example.com",
      "Port": 4040,
      "Location": {
        "City": "New York",
        "Country": "US",
        "Lat": 40.7123,
        "Lon": -74.0068
      },
      "AutonomousSystem": {
        "Name": "AnyCompany",
```

```

    "Number": 64496
  },
  "Connection": {
    "Direction": "INBOUND"
  }
}],
"Signals": [{
  "Id": "arn:aws:guardduty:us-east-1:123456789012:detector/
d0bfe135ab8b4dd8c3eaae7df9900073/finding/535a382b1bcc44d6b219517a29058fb7",
  "Title": "Someone ran a penetration test tool on your account.",
  "ActorIds": ["USER:AR0A987654321EXAMPLE:i-b188560f:1234567891"],
  "Count": 19,
  "FirstSeenAt": 1716916943000,
  "SignalIndicators": [
    {
      "Key": "ATTACK_TACTIC",
      "Title": "Attack Tactic",
      "Values": [
        "Impact"
      ]
    },
    {
      "Key": "HIGH_RISK_API",
      "Title": "High Risk Api",
      "Values": [
        "s3:DeleteObject"
      ]
    },
    {
      "Key": "ATTACK_TECHNIQUE",
      "Title": "Attack Technique",
      "Values": [
        "Data Destruction"
      ]
    }
  ],
  "LastSeenAt": 1716916944000,
  "Name": "Test:IAMUser/KaliLinux",
  "ResourceIds": [
    "arn:aws:s3:::amzn-s3-demo-destination-bucket"
  ],
  "Type": "FINDING"
}],
"SequenceIndicators": [

```

```
{
  "Key": "ATTACK_TACTIC",
  "Title": "Attack Tactic",
  "Values": [
    "Discovery",
    "Exfiltration",
    "Impact"
  ]
},
{
  "Key": "HIGH_RISK_API",
  "Title": "High Risk Api",
  "Values": [
    "s3:DeleteObject",
    "s3:GetObject",
    "s3:ListBuckets",
    "s3:ListObjects"
  ]
},
{
  "Key": "ATTACK_TECHNIQUE",
  "Title": "Attack Technique",
  "Values": [
    "Cloud Service Discovery",
    "Data Destruction"
  ]
}
]
```

FindingProviderFields

FindingProviderFieldsumfasst die folgenden Attribute:

- Confidence
- Criticality
- RelatedFindings
- Severity
- Types

Die obigen Felder sind unter dem `FindingProviderFields` Objekt verschachtelt, haben jedoch Entsprechungen mit demselben Namen wie ASFF-Felder der obersten Ebene. Wenn ein neuer Befund von einem Suchprovider an Security Hub CSPM gesendet wird, füllt Security Hub CSPM das `FindingProviderFields` Objekt automatisch auf, wenn es aufgrund der entsprechenden Felder der obersten Ebene leer ist.

Finding Provider können Updates `FindingProviderFields` mithilfe der [BatchImportFindings](#) Security Hub CSPM-API aktualisieren. Die Suche nach Anbietern kann dieses Objekt nicht mit aktualisieren. [BatchUpdateFindings](#)

Einzelheiten darüber, wie Security Hub CSPM Updates von `BatchImportFindings` zu `FindingProviderFields` und zu den entsprechenden Attributen der obersten Ebene verarbeitet, finden Sie unter. [the section called “Aktualisierung der Ergebnisse mit FindingProviderFields”](#)

Kunden können die Felder der obersten Ebene mithilfe des Vorgangs aktualisieren. `BatchUpdateFindings` Kunden können nicht aktualisieren `FindingProviderFields`.

Beispiel

```
"FindingProviderFields": {
  "Confidence": 42,
  "Criticality": 99,
  "RelatedFindings": [
    {
      "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "123e4567-e89b-12d3-a456-426655440000"
    }
  ],
  "Severity": {
    "Label": "MEDIUM",
    "Original": "MEDIUM"
  },
  "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

FirstObservedAt

Gibt an, wann das potenzielle Sicherheitsproblem oder das Ereignis, das durch einen Befund erfasst wurde, zum ersten Mal beobachtet wurde.

Dieser Zeitstempel gibt an, wann das Ereignis oder die Sicherheitsanfälligkeit zum ersten Mal beobachtet wurde. Folglich kann er vom `CreatedAt` Zeitstempel abweichen, der angibt, wann dieser Ergebnisdatensatz erstellt wurde.

Bei Kontrollergebnissen, die Security Hub CSPM generiert und aktualisiert, kann dieser Zeitstempel auch angeben, wann sich der Compliance-Status einer Ressource zuletzt geändert hat. Bei anderen Arten von Ergebnissen sollte dieser Zeitstempel zwischen Aktualisierungen des Ergebnisdatensatzes unveränderlich sein. Er kann jedoch aktualisiert werden, wenn ein genauerer Zeitstempel ermittelt wird.

Beispiel

```
"FirstObservedAt": "2017-03-22T13:22:13.933Z"
```

LastObservedAt

Gibt an, wann das potenzielle Sicherheitsproblem oder Ereignis, das durch ein Ergebnis erfasst wurde, zuletzt vom Produkt mit Sicherheitsergebnissen beobachtet wurde.

Dieser Zeitstempel gibt an, wann das Ereignis oder die Sicherheitsanfälligkeit zuletzt oder zuletzt beobachtet wurde. Folglich kann er vom `UpdatedAt` Zeitstempel abweichen, der angibt, wann dieser Ergebnisdatensatz zuletzt oder zuletzt aktualisiert wurde.

Sie können diesen Zeitstempel angeben, er ist jedoch bei der ersten Beobachtung nicht erforderlich. Wenn Sie dieses Feld bei der ersten Beobachtung ausfüllen, sollte der Zeitstempel mit dem Zeitstempel identisch sein. `FirstObservedAt` Sie sollten dieses Feld immer wieder aktualisieren, sodass immer der Zeitstempel der letzten Beobachtung des Fundes angegeben wird.

Beispiel

```
"LastObservedAt": "2017-03-23T13:22:13.933Z"
```

Schadsoftware

Das Objekt [Malware](#) stellt eine Liste der Malware zur Verfügung, die mit einem Fund zusammenhängt.

Beispiel

```
"Malware": [  
  {
```

```
    "Name": "Stringler",
    "Type": "COIN_MINER",
    "Path": "/usr/sbin/stringler",
    "State": "OBSERVED"
  }
]
```

Netzwerk (im Ruhestand)

Das [Network](#) Objekt stellt netzwerkbezogene Informationen zu einem Befund bereit.

Dieses Objekt ist ausgemustert. Um diese Daten bereitzustellen, können Sie die Daten entweder einer Ressource in zuordnen Resources oder das Action Objekt verwenden.

Beispiel

```
"Network": {
  "Direction": "IN",
  "OpenPortRange": {
    "Begin": 443,
    "End": 443
  },
  "Protocol": "TCP",
  "SourceIPv4": "1.2.3.4",
  "SourceIPv6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
  "SourcePort": "42",
  "SourceDomain": "example1.com",
  "SourceMac": "00:0d:83:b1:c0:8e",
  "DestinationIPv4": "2.3.4.5",
  "DestinationIPv6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
  "DestinationPort": "80",
  "DestinationDomain": "example2.com"
}
```

NetworkPath

Das [NetworkPath](#) Objekt stellt Informationen über einen Netzwerkpfad bereit, der mit einem Befund zusammenhängt. Jeder Eintrag in NetworkPath steht für eine Komponente des Pfads.

Beispiel

```
"NetworkPath" : [
  {
```



```

    "ComponentId": "abc-01a234bc56d8901ee",
    "ComponentType": "AWS::EC2::InternetGateway",
    "Egress": {
      "Destination": {
        "Address": [ "192.0.2.0/24" ],
        "PortRanges": [
          {
            "Begin": 443,
            "End": 443
          }
        ]
      },
      "Protocol": "TCP",
      "Source": {
        "Address": ["203.0.113.0/24"]
      }
    },
    "Ingress": {
      "Destination": {
        "Address": [ "198.51.100.0/24" ],
        "PortRanges": [
          {
            "Begin": 443,
            "End": 443
          }
        ]
      },
      "Protocol": "TCP",
      "Source": {
        "Address": [ "203.0.113.0/24" ]
      }
    }
  }
]

```

Hinweis

Das [Note](#) Objekt gibt eine benutzerdefinierte Notiz an, die Sie zu einem Ergebnis hinzufügen können.

Ein Ergebnisanbieter kann eine erste Notiz für ein Ergebnis bereitstellen, aber danach können keine Notizen hinzugefügt werden. Sie können eine Notiz nur mit [BatchUpdateFindings](#) aktualisieren.

Beispiel

```
"Note": {
  "Text": "Don't forget to check under the mat.",
  "UpdatedBy": "jsmith",
  "UpdatedAt": "2018-08-31T00:15:09Z"
}
```

PatchSummary

Das [PatchSummary](#) Objekt bietet eine Zusammenfassung des Patch-Konformitätsstatus einer Instanz anhand eines ausgewählten Konformitätsstandards.

Beispiel

```
"PatchSummary" : {
  "FailedCount" : 0,
  "Id" : "pb-123456789098",
  "InstalledCount" : 100,
  "InstalledOtherCount" : 1023,
  "InstalledPendingReboot" : 0,
  "InstalledRejectedCount" : 0,
  "MissingCount" : 100,
  "Operation" : "Install",
  "OperationEndTime" : "2018-09-27T23:39:31Z",
  "OperationStartTime" : "2018-09-27T23:37:31Z",
  "RebootOption" : "RebootIfNeeded"
}
```

Prozess

Das [Process](#) Objekt stellt prozessbezogene Details zu einem Ergebnis bereit.

Beispiel:

```
"Process": {
  "LaunchedAt": "2018-09-27T22:37:31Z",
  "Name": "syslogd",
  "ParentPid": 56789,
  "Path": "/usr/sbin/syslogd",
  "Pid": 12345,
  "TerminatedAt": "2018-09-27T23:37:31Z"
}
```

ProcessedAt

Zeigt an, wann Security Hub CSPM ein Ergebnis erhalten hat und mit dessen Verarbeitung begonnen hat.

Dies unterscheidet sich von `CreatedAt` und `UpdatedAt`, bei denen es sich um erforderliche Zeitstempel handelt, die sich auf die Interaktion des Ermittlungsanbieters mit dem Sicherheitsproblem und dem Ergebnis beziehen. Der `ProcessedAt` Zeitstempel gibt an, wann Security Hub CSPM mit der Verarbeitung eines Ergebnisses beginnt. Nach Abschluss der Verarbeitung wird ein Ergebnis im Konto eines Benutzers angezeigt.

```
"ProcessedAt": "2023-03-23T13:22:13.933Z"
```

ProductFields

Ein Datentyp, bei dem Produkte mit Sicherheitsergebnissen zusätzliche lösungsspezifische Details enthalten können, die nicht Teil des definierten AWS Sicherheitsfindungsformats sind.

Für Ergebnisse, die von Security Hub CSPM-Kontrollen generiert wurden, enthält `ProductFields` diese Informationen über die Kontrolle. Siehe [the section called “Generierung und Aktualisierung von Kontrollbefunden”](#).

Dieses Feld sollte keine redundanten Daten enthalten und darf keine Daten enthalten, die mit Feldern im AWS Security Finding Format in Konflikt stehen.

Das Präfix `aws/` steht für einen reservierten Namespace nur für AWS Produkte und Dienste und darf nicht zusammen mit Ergebnissen aus Integrationen von Drittanbietern eingereicht werden.

Auch wenn dies nicht unbedingt erforderlich ist, sollten Produkte Feldnamen wie folgt formatieren: `company-id/product-id/field-name`. Dabei sollten die `company-id` und `product-id` den Angaben im `ProductArn` des Fundes entsprechen.

Die Felder, auf die verwiesen wird, `Archival` werden verwendet, wenn Security Hub CSPM ein vorhandenes Ergebnis archiviert. Security Hub CSPM archiviert beispielsweise vorhandene Ergebnisse, wenn Sie eine Kontrolle oder einen Standard deaktivieren und wenn Sie [konsolidierte Kontrollergebnisse](#) ein- oder ausschalten.

Dieses Feld kann auch Informationen über den Standard enthalten, der die Kontrolle beinhaltet, die zu dem Ergebnis geführt hat.

Beispiel

```
"ProductFields": {
  "API", "DeleteTrail",
  "ArchivalReasons:0/Description": "The finding is in an ARCHIVED state because consolidated control findings has been turned on or off. This causes findings in the previous state to be archived when new findings are being generated.",
  "ArchivalReasons:0/ReasonCode": "CONSOLIDATED_CONTROL_FINDINGS_UPDATE",
  "aws/inspector/AssessmentTargetName": "My prod env",
  "aws/inspector/AssessmentTemplateName": "My daily CVE assessment",
  "aws/inspector/RulesPackageName": "Common Vulnerabilities and Exposures",
  "generico/secure-pro/Action.Type", "AWS_API_CALL",
  "generico/secure-pro/Count": "6",
  "Service_Name": "cloudtrail.amazonaws.com"
}
```

ProductName

Gibt den Namen des Produkts an, das den Befund generiert hat. Für Ergebnisse, die auf Kontrollen basieren, lautet der Produktname Security Hub CSPM.

Security Hub CSPM füllt dieses Attribut automatisch für jeden Befund aus. Sie können es nicht mit oder aktualisieren. [BatchImportFindingsBatchUpdateFindings](#) Die Ausnahme ist, wenn Sie eine benutzerdefinierte Integration verwenden. Siehe [the section called “Maßgeschneiderte Produktintegrationen”](#).

Wenn Sie die Security Hub CSPM-Konsole verwenden, um Ergebnisse nach Produktnamen zu filtern, verwenden Sie dieses Attribut.

Wenn Sie die Security Hub CSPM-API verwenden, um Ergebnisse nach Produktnamen zu filtern, verwenden Sie das `aws/securityhub/ProductName` Attribut unter `ProductFields`

Security Hub CSPM synchronisiert diese beiden Attribute nicht.

RecordState

Stellt den Datensatzstatus eines Ergebnisses bereit.

Standardmäßig werden Funde als ACTIVE erachtet, wenn sie anfangs von einem Service generiert werden.

Der Status ARCHIVED gibt an, dass ein Fund nicht mehr sichtbar sein sollte. Archivierte Ergebnisse werden nicht sofort gelöscht. Sie können sie suchen, überprüfen und darüber berichten. Security Hub

CSPM archiviert automatisch kontrollbasierte Ergebnisse, wenn die zugehörige Ressource gelöscht wird, die Ressource nicht existiert oder die Kontrolle deaktiviert ist.

RecordState ist für die Suche nach Anbietern vorgesehen und kann nur mithilfe dieses Vorgangs aktualisiert werden. [BatchImportFindings](#) Sie können es nicht mithilfe des [BatchUpdateFindings](#) Vorgangs aktualisieren.

Um den Status Ihrer Untersuchung zu einem Ergebnis nachzuverfolgen, verwenden Sie [Workflow](#) statt RecordState.

Wenn sich der Datensatzstatus von ARCHIVED zu ACTIVE ändert und der Workflow-Status des Ergebnisses NOTIFIED oder lautet RESOLVED, ändert Security Hub CSPM den Workflow-Status automatisch in. NEW

Beispiel

```
"RecordState": "ACTIVE"
```

Region

Gibt das an, AWS-Region aus dem das Ergebnis generiert wurde.

Security Hub CSPM füllt dieses Attribut automatisch für jeden Befund aus. Sie können es nicht mit oder aktualisieren. [BatchImportFindings](#) [BatchUpdateFindings](#)

Beispiel

```
"Region": "us-west-2"
```

RelatedFindings

Stellt eine Liste von Ergebnissen bereit, die sich auf das aktuelle Ergebnis beziehen.

RelatedFindings sollte nur mit der [BatchUpdateFindings](#) API-Operation aktualisiert werden. Sie sollten dieses Objekt nicht mit aktualisieren [BatchImportFindings](#).

Für [BatchImportFindings](#) Anfragen sollte die Suche nach Anbietern das RelatedFindings Objekt unter verwenden [FindingProviderFields](#).

Beschreibungen der RelatedFindings Attribute finden Sie [RelatedFinding](#) in der AWS Security Hub Cloud Security Posture Management (CSPM) API-Referenz.

Beispiel

```
"RelatedFindings": [
  { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
    "Id": "123e4567-e89b-12d3-a456-426655440000" },
  { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
    "Id": "AcmeNerfHerder-111111111111-x189dx7824" }
]
```

RiskAssessment

Beispiel

```
"RiskAssessment": {
  "Posture": {
    "FindingTotal": 4,
    "Indicators": [
      {
        "Type": "Reachability",
        "Findings": [
          {
            "Id": "arn:aws:inspector2:us-east-2:123456789012:finding/1234567890abcdef0",
            "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
            "Title": "Finding title"
          },
          {
            "Id": "arn:aws:inspector2:us-east-2:123456789012:finding/abcdef01234567890",
            "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
            "Title": "Finding title"
          }
        ]
      },
      {
        "Type": "Vulnerability",
        "Findings": [
          {
            "Id": "arn:aws:inspector2:us-east-2:123456789012:finding/021345abcdef6789",
```

```

        "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/
inspector",
        "Title": "Finding title"
    },
    {
        "Id": "arn:aws:inspector2:us-
east-2:123456789012:finding/021345ghijkl6789",
        "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/
inspector",
        "Title": "Finding title"
    }
]
}
}
}
}
}

```

Abhilfe

Das Objekt [Remediation](#) enthält Informationen zu empfohlenen Behebungsschritten für das Problem.

Beispiel

```

"Remediation": {
  "Recommendation": {
    "Text": "For instructions on how to fix this issue, see the AWS Security Hub
Cloud Security Posture Management (CSPM) documentation for EC2.2.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation"
  }
}

```

Beispiel

Gibt an, ob es sich bei dem Ergebnis um ein Beispielergebnis handelt.

```
"Sample": true
```

SourceUrl

Das `SourceUrl` Objekt stellt eine URL bereit, die auf eine Seite verweist, die sich mit dem aktuellen Ergebnis im gefundenen Produkt befasst.

```
"SourceUrl": "http://sourceurl.com"
```

ThreatIntelIndicators

Das [ThreatIntelIndicator](#) Objekt stellt Bedrohungsinformationen bereit, die sich auf einen Befund beziehen.

Beispiel

```
"ThreatIntelIndicators": [  
  {  
    "Category": "BACKDOOR",  
    "LastObservedAt": "2018-09-27T23:37:31Z",  
    "Source": "Threat Intel Weekly",  
    "SourceUrl": "http://threatintelweekly.org/backdoors/8888",  
    "Type": "IPV4_ADDRESS",  
    "Value": "8.8.8.8",  
  }  
]
```

Bedrohungen

Das [Threats](#) Objekt enthält Details zu der Bedrohung, die durch einen Befund erkannt wurde.

Beispiel

```
"Threats": [{  
  "FilePaths": [{  
    "FileName": "b.txt",  
    "FilePath": "/tmp/b.txt",  
    "Hash": "sha256",  
    "ResourceId": "arn:aws:ec2:us-west-2:123456789012:volume/vol-032f3bdd89aee112f"  
  }],  
  "ItemCount": 3,  
  "Name": "Iot.linux.mirai.vwisi",  
  "Severity": "HIGH"  
}]
```


UserDefinedFields

Stellt eine Liste von Zeichenfolgenpaaren aus Name und Wert bereit, die dem Befund zugeordnet sind. Dies sind individuelle, benutzerdefinierte Felder, die einem Fund hinzugefügt werden. Diese Felder können anhand Ihrer spezifischen Konfiguration automatisch generiert werden.

Bei der Suche nach Anbietern sollte dieses Feld nicht für Daten verwendet werden, die das Produkt generiert. Stattdessen kann das `ProductFields` Feld bei der Suche nach Anbietern für Daten verwendet werden, die keinem Standardfeld im Format für AWS Sicherheitssuche zugeordnet sind.

Diese Felder können nur mit [BatchUpdateFindings](#) aktualisiert werden.

Beispiel

```
"UserDefinedFields": {
  "reviewedByCio": "true",
  "comeBackToLater": "Check this again on Monday"
}
```

VerificationState

Stellt den Wahrheitsgehalt eines Ergebnisses sicher. Finds-Produkte können UNKNOWN für dieses Feld einen Wert von angeben. Ein Ergebnisprodukt sollte einen Wert für dieses Feld liefern, wenn das System des Ergebnisprodukts ein aussagekräftiges Analogon enthält. Dieses Feld wird in der Regel durch eine Benutzerentscheidung oder eine Aktion nach der Untersuchung eines Ergebnisses gefüllt.

Ein Ergebnisanbieter kann einen Anfangswert für dieses Attribut bereitstellen, es danach aber nicht aktualisieren. Sie können dieses Attribut nur aktualisieren, indem Sie [BatchUpdateFindings](#).

```
"VerificationState": "Confirmed"
```

Schwachstellen

Das [Vulnerabilities](#) Objekt enthält eine Liste von Sicherheitslücken, die mit einem Befund verknüpft sind.

Beispiel

```
"Vulnerabilities" : [
  {
```

```

"CodeVulnerabilities": [{
  "Cwes": [
    "CWE-798",
    "CWE-799"
  ],
  "FilePath": {
    "EndLine": 421,
    "FileName": "package-lock.json",
    "FilePath": "package-lock.json",
    "StartLine": 420
  },
  "SourceArn": "arn:aws:lambda:us-east-1:123456789012:layer:AWS-AppConfig-
Extension:114"
}],
"Cvss": [
  {
    "BaseScore": 4.7,
    "BaseVector": "AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N",
    "Version": "V3"
  },
  {
    "BaseScore": 4.7,
    "BaseVector": "AV:L/AC:M/Au:N/C:C/I:N/A:N",
    "Version": "V2"
  }
],
"EpssScore": 0.015,
"ExploitAvailable": "YES",
"FixAvailable": "YES",
"Id": "CVE-2020-12345",
"LastKnownExploitAt": "2020-01-16T00:01:35Z",
"ReferenceUrls": [
  "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12418",
  "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17563"
],
"RelatedVulnerabilities": ["CVE-2020-12345"],
"Vendor": {
  "Name": "Alas",
  "Url": "https://alas.aws.amazon.com/ALAS-2020-1337.html",
  "VendorCreatedAt": "2020-01-16T00:01:43Z",
  "VendorSeverity": "Medium",
  "VendorUpdatedAt": "2020-01-16T00:01:43Z"
},
"VulnerablePackages": [

```

```

    {
      "Architecture": "x86_64",
      "Epoch": "1",
      "FilePath": "/tmp",
      "FixedInVersion": "0.14.0",
      "Name": "openssl",
      "PackageManager": "OS",
      "Release": "16.amzn2.0.3",
      "Remediation": "Update aws-crt to 0.14.0",
      "SourceLayerArn": "arn:aws:lambda:us-west-2:123456789012:layer:id",
      "SourceLayerHash":
        "sha256:c1962c35b63a6ff6ce7df6e042ee82371a605ca9515569edec46ff14f926f001",
      "Version": "1.0.2k"
    }
  ]
}
]

```

Workflow

Das [Workflow](#)-Objekt bietet Informationen über den Status der Untersuchung zu einem Ergebnis.

Dieses Feld ist für Kunden zur Verwendung mit Tools zur Problembehebung, Orchestrierung und Ticketausstellung vorgesehen. Es ist nicht für die Suche nach Anbietern bestimmt.

Sie können das Feld nur mit aktualisieren. Workflow [BatchUpdateFindings](#) Kunden können ihn auch über die Konsole aktualisieren. Siehe [the section called “Den Workflow-Status von Ergebnissen festlegen”](#).

Beispiel

```

"Workflow": {
  "Status": "NEW"
}

```

WorkflowState (Im Ruhestand)

Dieses Objekt ist ausgemustert und wurde durch das Status Feld des Workflow Objekts ersetzt.

Dieses Feld gibt den Workflow-Status eines Ergebnisses an. Funde generierende Produkte können in diesem Feld den Wert NEW angeben. Ein Funde generierendes Produkte kann einen Wert in diesem Feld angeben, wenn es ein aussagekräftiges Analogon im System des Produkts gibt.

Beispiel

```
"WorkflowState": "NEW"
```

ResourcesASFF-Objekt

Im AWS Security Finding Format (ASFF) stellt das `Resources` Objekt Informationen zu den Ressourcen bereit, die an einem Befund beteiligt waren. Es enthält ein Array von bis zu 32 Ressourcenobjekten. Informationen zur Formatierung von Ressourcennamen finden Sie unter [AWS Format für Sicherheitssuche \(ASFF\)](#). Beispiele für jedes Ressourcenobjekt finden Sie, wenn Sie eine Ressource aus der folgenden Liste auswählen.

Themen

- [Ressourcenattribute im ASFF](#)
- [AwsAmazonMQRessourcen in ASFF](#)
- [AwsApiGatewayRessourcen in ASFF](#)
- [AwsAppSyncRessourcen in ASFF](#)
- [AwsAthenaRessourcen in ASFF](#)
- [AwsAutoScalingRessourcen in ASFF](#)
- [AwsBackupRessourcen in ASFF](#)
- [AwsCertificateManagerRessourcen in ASFF](#)
- [AwsCloudFormationRessourcen in ASFF](#)
- [AwsCloudFrontRessourcen in ASFF](#)
- [AwsCloudTrailRessourcen in ASFF](#)
- [AwsCloudWatchRessourcen in ASFF](#)
- [AwsCodeBuildRessourcen in ASFF](#)
- [AwsDmsRessourcen in ASFF](#)
- [AwsDynamoDBRessourcen in ASFF](#)
- [AwsEc2Ressourcen in ASFF](#)
- [AwsEcrRessourcen in ASFF](#)
- [AwsEcsRessourcen in ASFF](#)
- [AwsEfsRessourcen in ASFF](#)
- [AwsEksRessourcen in ASFF](#)

- [AwsElasticBeanstalkRessourcen in ASFF](#)
- [AwsElasticSearchRessourcen in ASFF](#)
- [AwsElbRessourcen in ASFF](#)
- [AwsEventBridgeRessourcen in ASFF](#)
- [AwsGuardDutyRessourcen in ASFF](#)
- [AwsIamRessourcen in ASFF](#)
- [AwsKinesisRessourcen in ASFF](#)
- [AwsKmsRessourcen in ASFF](#)
- [AwsLambda](#)
- [AwsMskRessourcen in ASFF](#)
- [AwsNetworkFirewallRessourcen in ASFF](#)
- [AwsOpenSearchServiceRessourcen in ASFF](#)
- [AwsRdsRessourcen in ASFF](#)
- [AwsRedshiftRessourcen in ASFF](#)
- [AwsRoute53Ressourcen in ASFF](#)
- [AwsS3Ressourcen in ASFF](#)
- [AwsSageMakerRessourcen in ASFF](#)
- [AwsSecretsManagerRessourcen in ASFF](#)
- [AwsSnsRessourcen in ASFF](#)
- [AwsSqsRessourcen in ASFF](#)
- [AwsSsmRessourcen in ASFF](#)
- [AwsStepFunctionsRessourcen in ASFF](#)
- [AwsWafRessourcen in ASFF](#)
- [AwsXrayRessourcen in ASFF](#)
- [ContainerASFF-Objekt](#)
- [OtherASFF-Objekt](#)

Ressourcenattribute im ASFF

Hier finden Sie Beschreibungen und Beispiele für das Resources Objekt im AWS Security Finding Format (ASFF). Weitere Informationen zu diesen Feldern finden Sie unter [Ressourcen](#).

ApplicationArn

Identifiziert den Amazon-Ressourcennamen (ARN) der Anwendung, die an der Suche beteiligt war.

Beispiel

```
"ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/SampleApp/1234567890abcdef0"
```

ApplicationName

Identifiziert den Namen der Anwendung, die an der Entdeckung beteiligt war.

Beispiel

```
"ApplicationName": "SampleApp"
```

DataClassification

Das [DataClassification](#)-Feld enthält Informationen über vertrauliche Daten, die auf der Ressource erkannt wurden.

Beispiel

```
"DataClassification": {
  "DetailedResultsLocation": "Path_to_Folder_Or_File",
  "Result": {
    "MimeType": "text/plain",
    "SizeClassified": 2966026,
    "AdditionalOccurrences": false,
    "Status": {
      "Code": "COMPLETE",
      "Reason": "Unsupportedfield"
    }
  },
  "SensitiveData": [
    {
      "Category": "PERSONAL_INFORMATION",
      "Detections": [
        {
          "Count": 34,
          "Type": "GE_PERSONAL_ID",
          "Occurrences": {
            "LineRanges": [
```

```

        {
            "Start": 1,
            "End": 10,
            "StartColumn": 20
        }
    ],
    "Pages": [],
    "Records": [],
    "Cells": []
}
},
{
    "Count": 59,
    "Type": "EMAIL_ADDRESS",
    "Occurrences": {
        "Pages": [
            {
                "PageNumber": 1,
                "OffsetRange": {
                    "Start": 1,
                    "End": 100,
                    "StartColumn": 10
                },
                "LineRange": {
                    "Start": 1,
                    "End": 100,
                    "StartColumn": 10
                }
            }
        ]
    }
},
{
    "Count": 2229,
    "Type": "URL",
    "Occurrences": {
        "LineRanges": [
            {
                "Start": 1,
                "End": 13
            }
        ]
    }
},

```

```

        {
            "Count": 13826,
            "Type": "NameDetection",
            "Occurrences": {
                "Records": [
                    {
                        "RecordIndex": 1,
                        "JsonPath": "$.ssn.value"
                    }
                ]
            }
        },
        {
            "Count": 32,
            "Type": "AddressDetection"
        }
    ],
    "TotalCount": 32
},
"CustomDataIdentifiers": {
    "Detections": [
        {
            "Arn": "1712be25e7c7f53c731fe464f1c869b8",
            "Name": "1712be25e7c7f53c731fe464f1c869b8",
            "Count": 2,
        }
    ],
    "TotalCount": 2
}
}
}

```

Details

Das [Details](#)-Feld enthält zusätzliche Informationen über eine einzelne Ressource, die die entsprechenden Objekte verwendet. Jede Ressource muss in einem separaten Ressourcenobjekt im `Resources`-Objekt bereitgestellt werden.

Beachten Sie, dass das `Details`-Objekt aus dem Ergebnis entfernt wird, wenn die Ergebnisgröße das Maximum von 240 KB überschreitet. Für Kontrollergebnisse, die AWS Config Regeln verwenden, können Sie sich die Ressourcendetails in der AWS Config Konsole ansehen.

Security Hub bietet eine Reihe verfügbarer Ressourcendetails für die unterstützten Ressourcentypen. Diese Details entsprechen den Werten des Type Objekts. Verwenden Sie nach Möglichkeit die bereitgestellten Typen.

Wenn es sich bei der Ressource beispielsweise um einen S3-Bucket handelt, legen Sie die Ressource Type auf fest `AwsS3Bucket` und geben Sie die Ressourcendetails im [AwsS3Bucket](#) Objekt an.

Mit dem [Other](#) Objekt können Sie benutzerdefinierte Felder und Werte angeben. Sie verwenden das `Other` Objekt in den folgenden Fällen:

- Der Ressourcentyp (der Wert der `ResourceType`) hat kein entsprechendes Detailobjekt. Um Details für die Ressource bereitzustellen, verwenden Sie das [Other](#) Objekt.
- Das Objekt für den Ressourcentyp enthält nicht alle Felder, die Sie auffüllen möchten. Verwenden Sie in diesem Fall das Detailobjekt für den Ressourcentyp, um die verfügbaren Felder auszufüllen. Verwenden Sie das `Other` Objekt, um die Felder aufzufüllen, die sich nicht im typspezifischen Objekt befinden.
- Der Ressourcentyp gehört nicht zu den angegebenen Typen. Stellen Sie in diesem Fall `Resource.Type` auf ein und verwenden Sie das `Other` Objekt `Other`, um die Details aufzufüllen.

Beispiel

```
"Details": {
  "AwsEc2Instance": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
    "ImageId": "ami-79fd7eee",
    "IPv4Addresses": ["1.1.1.1"],
    "IPv6Addresses": ["2001:db8:1234:1a2b::123"],
    "KeyName": "testkey",
    "LaunchedAt": "2018-09-29T01:25:54Z",
    "MetadataOptions": {
      "HttpEndpoint": "enabled",
      "HttpProtocolIpv6": "enabled",
      "HttpPutResponseHopLimit": 1,
      "HttpTokens": "optional",
      "InstanceMetadataTags": "disabled"
    },
    "NetworkInterfaces": [
      {
        "NetworkInterfaceId": "eni-e5aa89a3"
```

```
}  
],  
  "SubnetId": "PublicSubnet",  
  "Type": "i3.xlarge",  
  "VirtualizationType": "hvm",  
  "VpcId": "TestVPCIPv6"  
},  
  "AwsS3Bucket": {  
    "OwnerId": "da4d66eac431652a4d44d490a00500bde52c97d235b7b4752f9f688566fe6de",  
    "OwnerName": "acmes3bucketowner"  
  },  
  "Other": { "LightPen": "blinky", "SerialNo": "1234abcd"}  
}
```

Id

Der Bezeichner für den angegebenen Ressourcentyp.

Für AWS Ressourcen, die durch Amazon Resource Names (ARNs) identifiziert werden, ist dies der ARN.

Für AWS Ressourcen, die fehlen ARNs, ist dies die Kennung, wie sie von dem AWS Service definiert wurde, der die Ressource erstellt hat.

Bei AWS Nicht-Ressourcen ist dies eine eindeutige Kennung, die der Ressource zugeordnet ist.

Beispiel

```
"Id": "arn:aws:s3:::amzn-s3-demo-bucket"
```

Partition

Die Partition, in der sich die Ressource befindet. Eine Partition ist eine Gruppe von AWS-Regionen. Jede AWS-Konto ist auf eine Partition beschränkt.

Die folgenden Partitionen werden unterstützt:

- aws – AWS-Regionen
- aws-cn – China-Regionen
- aws-us-gov – AWS GovCloud (US) Region

Beispiel

```
"Partition": "aws"
```

Region

Der Code für den AWS-Region Ort, an dem sich diese Ressource befindet. Eine Liste der Regionscodes finden Sie unter [Regionale Endpunkte](#).

Beispiel

```
"Region": "us-west-2"
```

ResourceRole

Identifiziert die Rolle der Ressource bei dem Ergebnis. Eine Ressource ist entweder das Ziel der Suchaktivität oder der Akteur, der die Aktivität ausgeführt hat.

Beispiel

```
"ResourceRole": "target"
```

Tags

Dieses Feld enthält Informationen zu Schlüsselwörtern und Werten für die Ressource, die an einem Ergebnis beteiligt war. Sie können [Ressourcen taggen, die vom GetResources Betrieb der AWS Resource Groups Tagging-API unterstützt werden](#). Security Hub ruft diesen Vorgang über die [dienstverknüpfte Rolle](#) auf und ruft die Ressourcen-Tags ab, wenn das Resource.Id Feld AWS Security Finding Format (ASFF) mit dem AWS Ressourcen-ARN gefüllt ist. Ungültige Ressourcen IDs werden ignoriert.

Sie können Ressourcen-Tags zu Ergebnissen hinzufügen, die Security Hub aufnimmt, einschließlich Ergebnissen aus integrierten Produkten AWS-Services und Produkten von Drittanbietern.

Wenn Sie Tags hinzufügen, erfahren Sie, welche Tags einer Ressource zum Zeitpunkt der Verarbeitung des Ergebnisses zugeordnet waren. Sie können das Tags Attribut nur für Ressourcen einbeziehen, denen ein Tag zugeordnet ist. Wenn eine Ressource keine zugeordneten Tags hat, beziehen Sie beim Fund kein Tags-Attribut mit ein.

Durch die Aufnahme von Ressourcen-Tags in die Ergebnisse entfällt die Notwendigkeit, Pipelines zur Datenanreicherung zu erstellen oder die Metadaten von Sicherheitsergebnissen manuell

anzureichern. Sie können Tags auch verwenden, um Ergebnisse und Erkenntnisse zu suchen oder zu filtern und [Automatisierungsregeln](#) zu erstellen.

Informationen zu Einschränkungen, die für Tags gelten, finden Sie unter [Einschränkungen und Anforderungen für die Benennung von Tags](#).

In diesem Feld können Sie nur Tags angeben, die auf einer AWS Ressource vorhanden sind. Verwenden Sie das Unterfeld „OtherDetails“, um Daten bereitzustellen, die nicht im AWS Security Finding Format definiert sind.

Beispiel

```
"Tags": {
  "billingCode": "Lotus-1-2-3",
  "needsPatching": "true"
}
```

Typ

Der Ressourcentyp, für den Sie Details angeben.

Verwenden Sie nach Möglichkeit einen der bereitgestellten Ressourcentypen, z. B. `AwsEc2Instance` oder `AwsS3Bucket`.

Wenn der Ressourcentyp keinem der angegebenen Ressourcentypen entspricht, legen Sie die Ressource Type auf `Other` fest und füllen Sie die `Other Details` im Unterfeld „Details“ aus.

[Unterstützte Werte sind unter Ressourcen aufgeführt.](#)

Beispiel

```
"Type": "AwsS3Bucket"
```

AwsAmazonMQRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsAmazonMQ` Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter. [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsAmazonMQBroker

AwsAmazonMQBroker bietet Informationen über einen Amazon MQ-Broker, eine Message-Broker-Umgebung, die auf Amazon MQ ausgeführt wird.

Das folgende Beispiel zeigt den ASFF für das Objekt. `AwsAmazonMQBroker` Beschreibungen der `AwsAmazonMQBroker` Attribute finden Sie [AwsAmazonMQBroker](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsAmazonMQBroker": {
  "AutoMinorVersionUpgrade": true,
  "BrokerArn": "arn:aws:mq:us-east-1:123456789012:broker:TestBroker:b-
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "BrokerId": "b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "BrokerName": "TestBroker",
  "Configuration": {
    "Id": "c-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "Revision": 1
  },
  "DeploymentMode": "ACTIVE_STANDBY_MULTI_AZ",
  "EncryptionOptions": {
    "UseAwsOwnedKey": true
  },
  "EngineType": "ActiveMQ",
  "EngineVersion": "5.17.2",
  "HostInstanceType": "mq.t2.micro",
  "Logs": {
    "Audit": false,
    "AuditLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/
audit",
    "General": false,
    "GeneralLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111/general"
  },
  "MaintenanceWindowStartTime": {
    "DayOfWeek": "MONDAY",
    "TimeOfDay": "22:00",
    "TimeZone": "UTC"
  },
  "PubliclyAccessible": true,
  "SecurityGroups": [
```

```

    "sg-021345abcdef6789"
  ],
  "StorageType": "efs",
  "SubnetIds": [
    "subnet-1234567890abcdef0",
    "subnet-abcdef01234567890"
  ],
  "Users": [
    {
      "Username": "admin"
    }
  ]
}

```

AwsApiGatewayRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für AwsApiGateway Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter. [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsApiGatewayRestApi

Das AwsApiGatewayRestApi Objekt enthält Informationen über eine REST-API in Version 1 von Amazon API Gateway.

Im Folgenden finden Sie ein Beispiel für einen AwsApiGatewayRestApi Befund im AWS Security Finding Format (ASFF). Beschreibungen der AwsApiGatewayRestApi Attribute finden Sie [AwsApiGatewayRestApiDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```

AwsApiGatewayRestApi: {
  "Id": "exampleapi",
  "Name": "Security Hub",
  "Description": "AWS Security Hub",
  "CreateDate": "2018-11-18T10:20:05-08:00",
  "Version": "2018-10-26",
  "BinaryMediaTypes" : ["-*~1*"],
  "MinimumCompressionSize": 1024,
  "ApiKeySource": "AWS_ACCOUNT_ID",

```

```

    "EndpointConfiguration": {
      "Types": [
        "REGIONAL"
      ]
    }
  }
}

```

AwsApiGatewayStage

Das `AwsApiGatewayStage` Objekt stellt Informationen zu einer Amazon API Gateway Gateway-Stufe der Version 1 bereit.

Im Folgenden finden Sie ein Beispiel für einen `AwsApiGatewayStage` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsApiGatewayStage` Attribute finden Sie [AwsApiGatewayStageDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsApiGatewayStage": {
  "DeploymentId": "n7hlmf",
  "ClientCertificateId": "a1b2c3",
  "StageName": "Prod",
  "Description" : "Stage Description",
  "CacheClusterEnabled": false,
  "CacheClusterSize" : "1.6",
  "CacheClusterStatus": "NOT_AVAILABLE",
  "MethodSettings": [
    {
      "MetricsEnabled": true,
      "LoggingLevel": "INFO",
      "DataTraceEnabled": false,
      "ThrottlingBurstLimit": 100,
      "ThrottlingRateLimit": 5.0,
      "CachingEnabled": false,
      "CacheTtlInSeconds": 300,
      "CacheDataEncrypted": false,
      "RequireAuthorizationForCacheControl": true,
      "UnauthorizedCacheControlHeaderStrategy": "SUCCEED_WITH_RESPONSE_HEADER",
      "HttpMethod": "POST",
      "ResourcePath": "/echo"
    }
  ],
  "Variables": {"test": "value"},

```

```

    "DocumentationVersion": "2.0",
    "AccessLogSettings": {
        "Format": "{\\"requestId\\": \\"$context.requestId\\", \\"extendedRequestId\\": \\"$context.extendedRequestId\\", \\"ownerAccountId\\": \\"$context.accountId\\", \\"requestAccountId\\": \\"$context.identity.accountId\\", \\"callerPrincipal\\": \\"$context.identity.caller\\", \\"httpMethod\\": \\"$context.httpMethod\\", \\"resourcePath\\": \\"$context.resourcePath\\", \\"status\\": \\"$context.status\\", \\"requestTime\\": \\"$context.requestTime\\", \\"responseLatencyMs\\": \\"$context.responseLatency\\", \\"errorMessage\\": \\"$context.error.message\\", \\"errorResponseType\\": \\"$context.error.responseType\\", \\"apiId\\": \\"$context.apiId\\", \\"awsEndpointRequestId\\": \\"$context.awsEndpointRequestId\\", \\"domainName\\": \\"$context.domainName\\", \\"stage\\": \\"$context.stage\\", \\"xrayTraceId\\": \\"$context.xrayTraceId\\", \\"sourceIp\\": \\"$context.identity.sourceIp\\", \\"user\\": \\"$context.identity.user\\", \\"userAgent\\": \\"$context.identity.userAgent\\", \\"userArn\\": \\"$context.identity.userArn\\", \\"integrationLatency\\": \\"$context.integrationLatency\\", \\"integrationStatus\\": \\"$context.integrationStatus\\", \\"authorizerIntegrationLatency\\": \\"$context.authorizer.integrationLatency\\"}",
        "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-group:SecurityHubAPIAccessLog/Prod"
    },
    "CanarySettings": {
        "PercentTraffic": 0.0,
        "DeploymentId": "ul73s8",
        "StageVariableOverrides" : [
            "String" : "String"
        ],
        "UseStageCache": false
    },
    "TracingEnabled": false,
    "CreatedDate": "2018-07-11T10:55:18-07:00",
    "LastUpdatedDate": "2020-08-26T11:51:04-07:00",
    "WebAclArn" : "arn:aws:waf-regional:us-west-2:111122223333:webacl/cb606bd8-5b0b-4f0b-830a-dd304e48a822"
}

```

AwsApiGatewayV2Api

Das `AwsApiGatewayV2Api` Objekt enthält Informationen über eine API der Version 2 in Amazon API Gateway.

Im Folgenden finden Sie ein Beispiel für einen `AwsApiGatewayV2Api` Befund im AWS Security Finding Format (ASFF). Beschreibungen von `AwsApiGatewayV2Api` Attributen finden Sie unter [AwsApiGatewayV2 ApiDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsApiGatewayV2Api": {
  "ApiEndpoint": "https://example.us-west-2.amazonaws.com",
  "ApiId": "a1b2c3d4",
  "ApiKeySelectionExpression": "$request.header.x-api-key",
  "CreateDate": "2020-03-28T00:32:37Z",
  "Description": "ApiGatewayV2 Api",
  "Version": "string",
  "Name": "my-api",
  "ProtocolType": "HTTP",
  "RouteSelectionExpression": "$request.method $request.path",
  "CorsConfiguration": {
    "AllowOrigins": [ "*" ],
    "AllowCredentials": true,
    "ExposeHeaders": [ "string" ],
    "MaxAge": 3000,
    "AllowMethods": [
      "GET",
      "PUT",
      "POST",
      "DELETE",
      "HEAD"
    ],
    "AllowHeaders": [ "*" ]
  }
}
```

AwsApiGatewayV2-Stufe

`AwsApiGatewayV2Stage` enthält Informationen über eine Version 2-Stufe für Amazon API Gateway.

Im Folgenden finden Sie ein Beispiel für einen `AwsApiGatewayV2Stage` Befund im AWS Security Finding Format (ASFF). Beschreibungen von `AwsApiGatewayV2Stage` Attributen finden Sie unter [AwsApiGatewayV2 StageDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsApiGatewayV2Stage": {
  "CreateDate": "2020-04-08T00:36:05Z",
  "Description": "ApiGatewayV2",
  "DefaultRouteSettings": {
    "DetailedMetricsEnabled": false,
```

```

    "LoggingLevel": "INFO",
    "DataTraceEnabled": true,
    "ThrottlingBurstLimit": 100,
    "ThrottlingRateLimit": 50
  },
  "DeploymentId": "x1zwyv",
  "LastUpdatedDate": "2020-04-08T00:36:13Z",
  "RouteSettings": {
    "DetailedMetricsEnabled": false,
    "LoggingLevel": "INFO",
    "DataTraceEnabled": true,
    "ThrottlingBurstLimit": 100,
    "ThrottlingRateLimit": 50
  },
  "StageName": "prod",
  "StageVariables": [
    "function": "my-prod-function"
  ],
  "AccessLogSettings": {
    "Format": "{\"requestId\": \"${context.requestId}\", \"extendedRequestId\": \"${context.extendedRequestId}\", \"ownerAccountId\": \"${context.accountId}\", \"requestAccountId\": \"${context.identity.accountId}\", \"callerPrincipal\": \"${context.identity.caller}\", \"httpMethod\": \"${context.httpMethod}\", \"resourcePath\": \"${context.resourcePath}\", \"status\": \"${context.status}\", \"requestTime\": \"${context.requestTime}\", \"responseLatencyMs\": \"${context.responseLatency}\", \"errorMessage\": \"${context.error.message}\", \"errorResponseType\": \"${context.error.responseType}\", \"apiId\": \"${context.apiId}\", \"awsEndpointRequestId\": \"${context.awsEndpointRequestId}\", \"domainName\": \"${context.domainName}\", \"stage\": \"${context.stage}\", \"xrayTraceId\": \"${context.xrayTraceId}\", \"sourceIp\": \"${context.identity.sourceIp}\", \"user\": \"${context.identity.user}\", \"userAgent\": \"${context.identity.userAgent}\", \"userArn\": \"${context.identity.userArn}\", \"integrationLatency\": \"${context.integrationLatency}\", \"integrationStatus\": \"${context.integrationStatus}\", \"authorizerIntegrationLatency\": \"${context.authorizer.integrationLatency}\" }",
    "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-group:SecurityHubAPIAccessLog/Prod"
  },
  "AutoDeploy": false,
  "LastDeploymentStatusMessage": "Message",
  "ApiGatewayManaged": true,
}

```

AwsAppSyncRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für AwsAppSync Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter. [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsAppSyncGraphQLApi

AwsAppSyncGraphQLApi bietet Informationen über eine AWS AppSync GraphQL-API, bei der es sich um ein Konstrukt der obersten Ebene für Ihre Anwendung handelt.

Das folgende Beispiel zeigt den ASFF für das Objekt. AwsAppSyncGraphQLApi Beschreibungen der AwsAppSyncGraphQLApi Attribute finden Sie [AwsAppSyncGraphQLApi](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsAppSyncGraphQLApi": {
  "AdditionalAuthenticationProviders": [
    {
      "AuthenticationType": "AWS_LAMBDA",
      "LambdaAuthorizerConfig": {
        "AuthorizerResultTtlInSeconds": 300,
        "AuthorizerUri": "arn:aws:lambda:us-east-1:123456789012:function:mylambdafunc"
      }
    },
    {
      "AuthenticationType": "AWS_IAM"
    }
  ],
  "ApiId": "021345abcdef6789",
  "Arn": "arn:aws:appsync:eu-central-1:123456789012:apis/021345abcdef6789",
  "AuthenticationType": "API_KEY",
  "Id": "021345abcdef6789",
  "LogConfig": {
    "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/service-role/appsync-graphqlapi-logs-eu-central-1",
    "ExcludeVerboseContent": true,
    "FieldLogLevel": "ALL"
  },
}
```

```
"Name": "My AppSync App",
"XrayEnabled": true,
}
```

AwsAthenaRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für AwsAthena Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsAthenaWorkGroup

AwsAthenaWorkGroup bietet Informationen über eine Amazon Athena Athena-Arbeitsgruppe. Eine Arbeitsgruppe hilft Ihnen dabei, Benutzer, Teams, Anwendungen oder Workloads voneinander zu trennen. Sie hilft Ihnen auch dabei, Grenzen für die Datenverarbeitung festzulegen und die Kosten nachzuverfolgen.

Das folgende Beispiel zeigt den ASFF für das AwsAthenaWorkGroup Objekt. Beschreibungen der AwsAthenaWorkGroup Attribute finden Sie [AwsAthenaWorkGroup](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsAthenaWorkGroup": {
  "Description": "My workgroup for prod workloads",
  "Name": "MyWorkgroup",
  "WorkgroupConfiguration" {
    "ResultConfiguration": {
      "EncryptionConfiguration": {
        "EncryptionOption": "SSE_KMS",
        "KmsKey": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
      }
    }
  },
  "State": "ENABLED"
}
```

AwsAutoScalingRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für AwsAutoScaling Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsAutoScalingAutoScalingGroup

Das AwsAutoScalingAutoScalingGroup Objekt enthält Details zu einer automatischen Skalierungsgruppe.

Im Folgenden finden Sie ein Beispiel für einen AwsAutoScalingAutoScalingGroup Befund im AWS Security Finding Format (ASFF). Beschreibungen der AwsAutoScalingAutoScalingGroup Attribute finden Sie [AwsAutoScalingAutoScalingGroupDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsAutoScalingAutoScalingGroup": {
  "CreatedTime": "2017-10-17T14:47:11Z",
  "HealthCheckGracePeriod": 300,
  "HealthCheckType": "EC2",
  "LaunchConfigurationName": "mylaunchconf",
  "LoadBalancerNames": [],
  "LaunchTemplate": {
    "LaunchTemplateId": "string",
    "LaunchTemplateName": "string",
    "Version": "string"
  },
  "MixedInstancesPolicy": {
    "InstancesDistribution": {
      "OnDemandAllocationStrategy": "prioritized",
      "OnDemandBaseCapacity": number,
      "OnDemandPercentageAboveBaseCapacity": number,
      "SpotAllocationStrategy": "lowest-price",
      "SpotInstancePools": number,
      "SpotMaxPrice": "string"
    },
    "LaunchTemplate": {
      "LaunchTemplateSpecification": {
        "LaunchTemplateId": "string",
        "LaunchTemplateName": "string",
```

```

        "Version": "string"
      },
      "CapacityRebalance": true,
      "Overrides": [
        {
          "InstanceType": "string",
          "WeightedCapacity": "string"
        }
      ]
    }
  }
}

```

AwsAutoScalingLaunchConfiguration

Das `AwsAutoScalingLaunchConfiguration` Objekt enthält Details zu einer Startkonfiguration.

Im Folgenden finden Sie ein Beispiel für einen `AwsAutoScalingLaunchConfiguration` Befund im AWS Security Finding Format (ASFF).

Beschreibungen der `AwsAutoScalingLaunchConfiguration` Attribute finden Sie [AwsAutoScalingLaunchConfigurationDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```

AwsAutoScalingLaunchConfiguration: {
  "LaunchConfigurationName": "newtest",
  "ImageId": "ami-058a3739b02263842",
  "KeyName": "55hundredinstance",
  "SecurityGroups": [ "sg-01fce87ad6e019725" ],
  "ClassicLinkVpcSecurityGroups": [],
  "UserData": "...Base64-Encoded user data..."
  "InstanceType": "a1.metal",
  "KernelId": "",
  "RamdiskId": "ari-a51cf9cc",
  "BlockDeviceMappings": [
    {
      "DeviceName": "/dev/sdh",
      "Ebs": {
        "VolumeSize": 30,
        "VolumeType": "gp2",
        "DeleteOnTermination": false,
        "Encrypted": true,

```

```

        "SnapshotId": "snap-ffaa1e69",
        "VirtualName": "ephemeral1"
    },
    {
        "DeviceName": "/dev/sdb",
        "NoDevice": true
    },
    {
        "DeviceName": "/dev/sda1",
        "Ebs": {
            "SnapshotId": "snap-02420cd3d2dea1bc0",
            "VolumeSize": 8,
            "VolumeType": "gp2",
            "DeleteOnTermination": true,
            "Encrypted": false
        }
    },
    {
        "DeviceName": "/dev/sdi",
        "Ebs": {
            "VolumeSize": 20,
            "VolumeType": "gp2",
            "DeleteOnTermination": false,
            "Encrypted": true
        }
    },
    {
        "DeviceName": "/dev/sdc",
        "NoDevice": true
    }
],
"InstanceMonitoring": {
    "Enabled": false
},
"CreatedTime": 1620842933453,
"EbsOptimized": false,
"AssociatePublicIpAddress": true,
"SpotPrice": "0.045"
}

```

AwsBackupRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für AwsBackup Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter. [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsBackupBackupPlan

Das AwsBackupBackupPlan Objekt stellt Informationen zu einem AWS Backup Backup-Plan bereit. Ein AWS Backup Backup-Plan ist ein Richtlinien Ausdruck, der definiert, wann und wie Sie Ihre AWS Ressourcen sichern möchten.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das AwsBackupBackupPlan Objekt. Beschreibungen der AwsBackupBackupPlan Attribute finden Sie [AwsBackupBackupPlan](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsBackupBackupPlan": {
  "BackupPlan": {
    "AdvancedBackupSettings": [{
      "BackupOptions": {
        "WindowsVSS": "enabled"
      },
      "ResourceType": "EC2"
    }],
    "BackupPlanName": "test",
    "BackupPlanRule": [{
      "CompletionWindowMinutes": 10080,
      "CopyActions": [{
        "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-vault:aws/efs/automatic-backup-vault",
        "Lifecycle": {
          "DeleteAfterDays": 365,
          "MoveToColdStorageAfterDays": 30
        }
      }],
      "Lifecycle": {
        "DeleteAfterDays": 35
      }
    }],
  },
}
```



```

    "RuleName": "DailyBackups",
    "ScheduleExpression": "cron(0 5 ? * * *)",
    "StartWindowMinutes": 480,
    "TargetBackupVault": "Default"
  },
  {
    "CompletionWindowMinutes": 10080,
    "CopyActions": [{
      "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
      "Lifecycle": {
        "DeleteAfterDays": 365,
        "MoveToColdStorageAfterDays": 30
      }
    }],
    "Lifecycle": {
      "DeleteAfterDays": 35
    },
    "RuleName": "Monthly",
    "ScheduleExpression": "cron(0 5 1 * ? *)",
    "StartWindowMinutes": 480,
    "TargetBackupVault": "Default"
  }
],
  "BackupPlanArn": "arn:aws:backup:us-east-1:858726136373:backup-
plan:b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
  "BackupPlanId": "b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
  "VersionId": "ZDVjNDIzMjItYTZiNS00NzczLTg4YzctNmExMWM2NjZhY2E1"
}

```

AwsBackupBackupVault

Das `AwsBackupBackupVault` Objekt stellt Informationen zu einem AWS Backup Backup-Tresor bereit. Ein AWS Backup Backup-Tresor ist ein Container, der Ihre Backups speichert und organisiert.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsBackupBackupVault` Objekt. Beschreibungen der `AwsBackupBackupVault` Attribute finden Sie [AwsBackupBackupVault](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsBackupBackupVault": {
  "AccessPolicy": {

```

```

"Statement": [{
  "Action": [
    "backup:DeleteBackupVault",
    "backup:DeleteBackupVaultAccessPolicy",
    "backup:DeleteRecoveryPoint",
    "backup:StartCopyJob",
    "backup:StartRestoreJob",
    "backup:UpdateRecoveryPointLifecycle"
  ],
  "Effect": "Deny",
  "Principal": {
    "AWS": "*"
  },
  "Resource": "*"
}],
"Version": "2012-10-17"
},
{
  "BackupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-vault:aws/efs/automatic-backup-vault",
  "BackupVaultName": "aws/efs/automatic-backup-vault",
  "EncryptionKeyArn": "arn:aws:kms:us-east-1:444455556666:key/72ba68d4-5e43-40b0-ba38-838bf8d06ca0",
  "Notifications": {
    "BackupVaultEvents": ["BACKUP_JOB_STARTED", "BACKUP_JOB_COMPLETED", "COPY_JOB_STARTED"],
    "SNSTopicArn": "arn:aws:sns:us-west-2:111122223333:MyVaultTopic"
  }
}
}

```

AwsBackupRecoveryPoint

Das `AwsBackupRecoveryPoint` Objekt stellt Informationen zu einer AWS Backup Sicherung bereit, die auch als Wiederherstellungspunkt bezeichnet wird. Ein AWS Backup Wiederherstellungspunkt stellt den Inhalt einer Ressource zu einem bestimmten Zeitpunkt dar.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsBackupRecoveryPoint` Objekt. Beschreibungen der `AwsBackupBackupVault` Attribute finden Sie [AwsBackupRecoveryPoint](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsBackupRecoveryPoint": {
  "BackupSizeInBytes": 0,

```

```

    "BackupVaultName": "aws/efs/automatic-backup-vault",
    "BackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/efs/automatic-backup-vault",
    "CalculatedLifecycle": {
      "DeleteAt": "2021-08-30T06:51:58.271Z",
      "MoveToColdStorageAt": "2020-08-10T06:51:58.271Z"
    },
    "CompletionDate": "2021-07-26T07:21:40.361Z",
    "CreatedBy": {
      "BackupPlanArn": "arn:aws:backup:us-east-1:111122223333:backup-plan:aws/efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
      "BackupPlanId": "aws/efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
      "BackupPlanVersion": "ZGM4YzY5YjktMWYxNC00ZTBmLWE5MjYtZmU5OWNiZmM5ZjIz",
      "BackupRuleId": "2a600c2-42ad-4196-808e-084923ebfd25"
    },
    "CreationDate": "2021-07-26T06:51:58.271Z",
    "EncryptionKeyArn": "arn:aws:kms:us-east-1:111122223333:key/72ba68d4-5e43-40b0-ba38-838bf8d06ca0",
    "IamRoleArn": "arn:aws:iam::111122223333:role/aws-service-role/backup.amazonaws.com/AWSServiceRoleForBackup",
    "IsEncrypted": true,
    "LastRestoreTime": "2021-07-26T06:51:58.271Z",
    "Lifecycle": {
      "DeleteAfterDays": 35,
      "MoveToColdStorageAfterDays": 15
    },
    "RecoveryPointArn": "arn:aws:backup:us-east-1:111122223333:recovery-point:151a59e4-f1d5-4587-a7fd-0774c6e91268",
    "ResourceArn": "arn:aws:elasticfilesystem:us-east-1:858726136373:file-system/fs-15bd31a1",
    "ResourceType": "EFS",
    "SourceBackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/efs/automatic-backup-vault",
    "Status": "COMPLETED",
    "StatusMessage": "Failure message",
    "StorageClass": "WARM"
  }
}

```

AwsCertificateManagerRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für AwsCertificateManager Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsCertificateManagerCertificate

Das `AwsCertificateManagerCertificate` Objekt enthält Details zu einem AWS Certificate Manager (ACM-) Zertifikat.

Im Folgenden finden Sie ein Beispiel für einen `AwsCertificateManagerCertificate` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsCertificateManagerCertificate` Attribute finden Sie [AwsCertificateManagerCertificateDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsCertificateManagerCertificate": {
  "CertificateAuthorityArn": "arn:aws:acm:us-west-2:444455556666:certificate-
authority/example",
  "CreatedAt": "2019-05-24T18:12:02.000Z",
  "DomainName": "example.amazondomains.com",
  "DomainValidationOptions": [
    {
      "DomainName": "example.amazondomains.com",
      "ResourceRecord": {
        "Name": "_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
        "Type": "CNAME",
        "Value": "_example.acm-validations.aws."
      },
      "ValidationDomain": "example.amazondomains.com",
      "ValidationEmails": [sample_email@sample.com],
      "ValidationMethod": "DNS",
      "ValidationStatus": "SUCCESS"
    }
  ],
  "ExtendedKeyUsages": [
    {
      "Name": "TLS_WEB_SERVER_AUTHENTICATION",
      "Oid": "1.3.6.1.5.5.7.3.1"
    },
    {
      "Name": "TLS_WEB_CLIENT_AUTHENTICATION",
      "Oid": "1.3.6.1.5.5.7.3.2"
    }
  ]
}
```

```

],
"FailureReason": "",
"ImportedAt": "2018-08-17T00:13:00.000Z",
"InUseBy": ["arn:aws:amazondomains:us-west-2:444455556666:loadbalancer/example"],
"IssuedAt": "2020-04-26T00:41:17.000Z",
"Issuer": "Amazon",
"KeyAlgorithm": "RSA-1024",
"KeyUsages": [
  {
    "Name": "DIGITAL_SIGNATURE",
  },
  {
    "Name": "KEY_ENCIPHERMENT",
  }
],
"NotAfter": "2021-05-26T12:00:00.000Z",
"NotBefore": "2020-04-26T00:00:00.000Z",
"Options": {
  "CertificateTransparencyLoggingPreference": "ENABLED",
}
"RenewalEligibility": "ELIGIBLE",
"RenewalSummary": {
  "DomainValidationOptions": [
    {
      "DomainName": "example.amazondomains.com",
      "ResourceRecord": {
        "Name":
"_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
        "Type": "CNAME",
        "Value": "_example.acm-validations.aws.com",
      },
      "ValidationDomain": "example.amazondomains.com",
      "ValidationEmails": ["sample_email@sample.com"],
      "ValidationMethod": "DNS",
      "ValidationStatus": "SUCCESS"
    }
  ],
  "RenewalStatus": "SUCCESS",
  "RenewalStatusReason": "",
  "UpdatedAt": "2020-04-26T00:41:35.000Z",
},
"Serial": "02:ac:86:b6:07:2f:0a:61:0e:3a:ac:fd:d9:ab:17:1a",
"SignatureAlgorithm": "SHA256WITHRSA",
"Status": "ISSUED",

```

```
"Subject": "CN=example.amazondomains.com",
"SubjectAlternativeNames": ["example.amazondomains.com"],
"Type": "AMAZON_ISSUED"
}
```

AwsCloudFormationRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für AwsCloudFormation Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter. [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsCloudFormationStack

Das AwsCloudFormationStack Objekt enthält Details zu einem AWS CloudFormation Stapel, der als Ressource in einer Vorlage der obersten Ebene verschachtelt ist.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt.

AwsCloudFormationStack Beschreibungen der AwsCloudFormationStack Attribute finden Sie [AwsCloudFormationStackDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsCloudFormationStack": {
  "Capabilities": [
    "CAPABILITY_IAM",
    "CAPABILITY_NAMED_IAM"
  ],
  "CreationTime": "2022-02-18T15:31:53.161Z",
  "Description": "AWS CloudFormation Sample",
  "DisableRollback": true,
  "DriftInformation": {
    "StackDriftStatus": "DRIFTED"
  },
  "EnableTerminationProtection": false,
  "LastUpdatedTime": "2022-02-18T15:31:53.161Z",
  "NotificationArns": [
    "arn:aws:sns:us-east-1:978084797471:sample-sns-cfn"
  ],
  "Outputs": [{
    "Description": "URL for newly created LAMP stack",
    "OutputKey": "WebsiteUrl",
```

```
"OutputValue": "http://ec2-44-193-18-241.compute-1.amazonaws.com"
}],
"RoleArn": "arn:aws:iam::012345678910:role/exampleRole",
"StackId": "arn:aws:cloudformation:us-east-1:978084797471:stack/sample-stack/
e5d9f7e0-90cf-11ec-88c6-12ac1f91724b",
"StackName": "sample-stack",
"StackStatus": "CREATE_COMPLETE",
"StackStatusReason": "Success",
"TimeoutInMinutes": 1
}
```

AwsCloudFrontRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für AwsCloudFront Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter. [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsCloudFrontDistribution

Das AwsCloudFrontDistribution Objekt enthält Details zu einer CloudFront Amazon-Vertriebskonfiguration.

Im Folgenden finden Sie ein Beispiel für einen AwsCloudFrontDistribution Befund im AWS Security Finding Format (ASFF). Beschreibungen der AwsCloudFrontDistribution Attribute finden Sie [AwsCloudFrontDistributionDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsCloudFrontDistribution": {
  "CacheBehaviors": {
    "Items": [
      {
        "ViewerProtocolPolicy": "https-only"
      }
    ]
  },
  "DefaultCacheBehavior": {
    "ViewerProtocolPolicy": "https-only"
  },
  "DefaultRootObject": "index.html",
  "DomainName": "d2wkuj2w9l34gt.cloudfront.net",
```

```

"Etag": "E37HOT42DHPVYH",
"LastModifiedTime": "2015-08-31T21:11:29.093Z",
"Logging": {
  "Bucket": "myawslogbucket.s3.amazonaws.com",
  "Enabled": false,
  "IncludeCookies": false,
  "Prefix": "myawslog/"
},
"OriginGroups": {
  "Items": [
    {
      "FailoverCriteria": {
        "StatusCodes": {
          "Items": [
            200,
            301,
            404
          ]
        }
      }
    }
  ]
},
"Origins": {
  "Items": [
    {
      "CustomOriginConfig": {
        "HttpPort": 80,
        "HttpsPort": 443,
        "OriginKeepaliveTimeout": 60,
        "OriginProtocolPolicy": "match-viewer",
        "OriginReadTimeout": 30,
        "OriginSslProtocols": {
          "Items": ["SSLv3", "TLSv1"],
          "Quantity": 2
        }
      }
    }
  ]
},
"DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
"Id": "my-origin",
"OriginPath": "/production",

```



```

        "S3OriginConfig": {
            "OriginAccessIdentity": "origin-access-identity/cloudfront/
E2YFS67H6VB6E4"
        }
    ],
    "Status": "Deployed",
    "ViewerCertificate": {
        "AcmCertificateArn": "arn:aws:acm::123456789012:AcmCertificateArn",
        "Certificate": "ASCAJRRE5XYF52TKRY5M4",
        "CertificateSource": "iam",
        "CloudFrontDefaultCertificate": true,
        "IamCertificateId": "ASCAJRRE5XYF52TKRY5M4",
        "MinimumProtocolVersion": "TLSv1.2_2021",
        "SslSupportMethod": "sni-only"
    },
    "WebAclId": "waf-1234567890"
}

```

AwsCloudTrailRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für AwsCloudTrail Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsCloudTrailTrail

Das AwsCloudTrailTrail Objekt liefert Details zu einer AWS CloudTrail Spur.

Im Folgenden finden Sie ein Beispiel für einen AwsCloudTrailTrail Befund im AWS Security Finding Format (ASFF). Beschreibungen der AwsCloudTrailTrail Attribute finden Sie [AwsCloudTrailTrailDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsCloudTrailTrail": {
    "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-west-2:123456789012:log-
group:CloudTrail/regression:*",
    "CloudWatchLogsRoleArn": "arn:aws:iam::866482105055:role/
CloudTrail_CloudWatchLogs",

```

```

    "HasCustomEventSelectors": true,
    "HomeRegion": "us-west-2",
    "IncludeGlobalServiceEvents": true,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "KmsKeyId": "kmsKeyId",
    "LogFileValidationEnabled": true,
    "Name": "regression-trail",
    "S3BucketName": "cloudtrail-bucket",
    "S3KeyPrefix": "s3KeyPrefix",
    "SnsTopicArn": "arn:aws:sns:us-east-2:123456789012:MyTopic",
    "SnsTopicName": "snsTopicName",
    "TrailArn": "arn:aws:cloudtrail:us-west-2:123456789012:trail"
  }

```

AwsCloudWatchRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für AwsCloudWatch Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter. [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsCloudWatchAlarm

Das AwsCloudWatchAlarm Objekt bietet Details zu CloudWatch Amazon-Alarmen, die eine Metrik beobachten oder eine Aktion ausführen, wenn sich der Status eines Alarms ändert.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das AwsCloudWatchAlarm Objekt. Beschreibungen der AwsCloudWatchAlarm Attribute finden Sie [AwsCloudWatchAlarmDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsCloudWatchAlarm": {
  "ActionsEnabled": true,
  "AlarmActions": [
    "arn:aws:automate:region:ec2:stop",
    "arn:aws:automate:region:ec2:terminate"
  ],
  "AlarmArn": "arn:aws:cloudwatch:us-west-2:012345678910:alarm:sampleAlarm",
  "AlarmConfigurationUpdatedTimestamp": "2022-02-18T15:31:53.161Z",

```

```

"AlarmDescription": "Alarm Example",
"AlarmName": "Example",
"ComparisonOperator": "GreaterThanOrEqualToThreshold",
"DatapointsToAlarm": 1,
"Dimensions": [{
  "Name": "InstanceId",
  "Value": "i-1234567890abcdef0"
}],
"EvaluateLowSampleCountPercentile": "evaluate",
"EvaluationPeriods": 1,
"ExtendedStatistic": "p99.9",
"InsufficientDataActions": [
  "arn:aws:automate:region:ec2:stop"
],
"MetricName": "Sample Metric",
"Namespace": "YourNamespace",
"OkActions": [
  "arn:aws:swf:region:account-id:action/actions/AWS_EC2.InstanceId.Stop/1.0"
],
"Period": 1,
"Statistic": "SampleCount",
"Threshold": 12.3,
"ThresholdMetricId": "t1",
"TreatMissingData": "notBreaching",
"Unit": "Kilobytes/Second"
}

```

AwsCodeBuildRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für AwsCodeBuild Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter. [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsCodeBuildProject

Das Objekt `AwsCodeBuildProject` liefert Informationen zu einem AWS CodeBuild -Projekt.

Im Folgenden finden Sie ein Beispiel für einen `AwsCodeBuildProject` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsCodeBuildProject` Attribute finden Sie [AwsCodeBuildProjectDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsCodeBuildProject": {
  "Artifacts": [
    {
      "ArtifactIdentifier": "string",
      "EncryptionDisabled": boolean,
      "Location": "string",
      "Name": "string",
      "NamespaceType": "string",
      "OverrideArtifactName": boolean,
      "Packaging": "string",
      "Path": "string",
      "Type": "string"
    }
  ],
  "SecondaryArtifacts": [
    {
      "ArtifactIdentifier": "string",
      "EncryptionDisabled": boolean,
      "Location": "string",
      "Name": "string",
      "NamespaceType": "string",
      "OverrideArtifactName": boolean,
      "Packaging": "string",
      "Path": "string",
      "Type": "string"
    }
  ],
  "EncryptionKey": "string",
  "Certificate": "string",
  "Environment": {
    "Certificate": "string",
    "EnvironmentVariables": [
      {
        "Name": "string",
        "Type": "string",
        "Value": "string"
      }
    ]
  },
  "ImagePullCredentialsType": "string",
  "PrivilegedMode": boolean,
  "RegistryCredential": {
    "Credential": "string",
```

```

    "CredentialProvider": "string"
  },
  "Type": "string"
},
"LogsConfig": {
  "CloudWatchLogs": {
    "GroupName": "string",
    "Status": "string",
    "StreamName": "string"
  },
  "S3Logs": {
    "EncryptionDisabled": boolean,
    "Location": "string",
    "Status": "string"
  }
},
"Name": "string",
"ServiceRole": "string",
"Source": {
  "Type": "string",
  "Location": "string",
  "GitCloneDepth": integer
},
"VpcConfig": {
  "VpcId": "string",
  "Subnets": ["string"],
  "SecurityGroupIds": ["string"]
}
}

```

AwsDmsRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für AwsDms Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter. [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsDmsEndpoint

Das AwsDmsEndpoint Objekt stellt Informationen über einen AWS Database Migration Service (AWS DMS) -Endpunkt bereit. Ein Endpunkt stellt Verbindungs-, Datenspeichertyp- und Standortinformationen zu Ihrem Datenspeicher bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsDmsEndpoint` Objekt. Beschreibungen der `AwsDmsEndpoint` Attribute finden Sie [AwsDmsEndpointDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsDmsEndpoint": {
  "CertificateArn": "arn:aws:dms:us-east-1:123456789012:cert:EXAMPLEIGDURVZGVJQZDPWJ5A7F2YDJVSMTBWFI",
  "DatabaseName": "Test",
  "EndpointArn": "arn:aws:dms:us-east-1:123456789012:endpoint:EXAMPLEQB3CZY33F7XV253NAJVBPNK6MJQVQVQA",
  "EndpointIdentifier": "target-db",
  "EndpointType": "TARGET",
  "EngineName": "mariadb",
  "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Port": 3306,
  "ServerName": "target-db.exampletafyu.us-east-1.rds.amazonaws.com",
  "SslMode": "verify-ca",
  "Username": "admin"
}
```

AwsDmsReplicationInstance

Das `AwsDmsReplicationInstance` Objekt stellt Informationen über eine AWS Database Migration Service (AWS DMS) Replikationsinstanz bereit. DMS verwendet eine Replikationsinstanz, um eine Verbindung zu Ihrem Quelldatenspeicher herzustellen, die Quelldaten zu lesen und die Daten für den Zieldatenspeicher zu formatieren.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsDmsReplicationInstance` Objekt. Beschreibungen der `AwsDmsReplicationInstance` Attribute finden Sie [AwsDmsReplicationInstanceDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsDmsReplicationInstance": {
  "AllocatedStorage": 50,
  "AutoMinorVersionUpgrade": true,
  "AvailabilityZone": "us-east-1b",
  "EngineVersion": "3.5.1",
}
```

```

    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "MultiAZ": false,
    "PreferredMaintenanceWindow": "wed:08:08-wed:08:38",
    "PubliclyAccessible": true,
    "ReplicationInstanceClass": "dms.c5.xlarge",
    "ReplicationInstanceIdentifier": "second-replication-instance",
    "ReplicationSubnetGroup": {
        "ReplicationSubnetGroupIdentifier": "default-vpc-2344f44f"
    },
    "VpcSecurityGroups": [
        {
            "VpcSecurityGroupId": "sg-003a34e205138138b"
        }
    ]
}

```

AwsDmsReplicationTask

Das `AwsDmsReplicationTask` Objekt stellt Informationen über eine AWS Database Migration Service (AWS DMS) Replikationsaufgabe bereit. Eine Replikationsaufgabe verschiebt einen Datensatz vom Quellendpunkt zum Zielendpunkt.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsDmsReplicationInstance` Objekt. Beschreibungen der `AwsDmsReplicationInstance` Attribute finden Sie [AwsDmsReplicationInstance](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsDmsReplicationTask": {
    "CdcStartPosition": "2023-08-28T14:26:22",
    "Id": "arn:aws:dms:us-east-1:123456789012:task:YDYU0HZIXWKQSUCBMUCQCN44SJW74VJNB5DFWQ",
    "MigrationType": "cdc",
    "ReplicationInstanceArn": "arn:aws:dms:us-east-1:123456789012:rep:T7V6RFDP23PYQWUL26N3PF5REKML4Y0UGIMYJUI",
    "ReplicationTaskIdentifier": "test-task",
    "ReplicationTaskSettings": "{\n\"Logging\":{\n\"EnableLogging\":false,\n\"EnableLogContext\":false,\n\"LogComponents\":[\n{\n\"Severity\":\n\"LOGGER_SEVERITY_DEFAULT\n\", \n\"Id\":\n\"TRANSFORMATION\n\"}, {\n\"Severity\":\n\"LOGGER_SEVERITY_DEFAULT\n\", \n\"Id\":\n\"SOURCE_UNLOAD\n\"}, {\n\"Severity\":\n\"LOGGER_SEVERITY_DEFAULT\n\", \n\"Id\":\n\"IO\n\"}, {\n\"Severity\":\n\"LOGGER_SEVERITY_DEFAULT\n\", \n\"Id\":\n\"TARGET_LOAD\n\"}, {\n\"Severity\":\n\"LOGGER_SEVERITY_DEFAULT\n\", \n\"Id\":\n\"PERFORMANCE\n\"}, {\n\"Severity

```

```

\":"LOGGER_SEVERITY_DEFAULT\","Id\":"SOURCE_CAPTURE\"},"Severity\":"
"LOGGER_SEVERITY_DEFAULT\","Id\":"SORTER\"},"Severity\":"LOGGER_SEVERITY_DEFAULT
\","Id\":"REST_SERVER\"},"Severity\":"LOGGER_SEVERITY_DEFAULT\","Id
\":"VALIDATOR_EXT\"},"Severity\":"LOGGER_SEVERITY_DEFAULT\","Id\":"
"TARGET_APPLY\"},"Severity\":"LOGGER_SEVERITY_DEFAULT\","Id\":"TASK_MANAGER
\"},"Severity\":"LOGGER_SEVERITY_DEFAULT\","Id\":"TABLES_MANAGER\"},"
{"Severity\":"LOGGER_SEVERITY_DEFAULT\","Id\":"METADATA_MANAGER\"},"
{"Severity\":"LOGGER_SEVERITY_DEFAULT\","Id\":"FILE_FACTORY\"},"Severity\":"
"LOGGER_SEVERITY_DEFAULT\","Id\":"COMMON\"},"Severity\":"LOGGER_SEVERITY_DEFAULT
\","Id\":"ADDONS\"},"Severity\":"LOGGER_SEVERITY_DEFAULT\","Id\":"DATA_STRUCTURE
\"},"Severity\":"LOGGER_SEVERITY_DEFAULT\","Id\":"COMMUNICATION\"},"Severity
\":"LOGGER_SEVERITY_DEFAULT\","Id\":"FILE_TRANSFER\"]},"CloudWatchLogGroup
\":"null","CloudWatchLogStream\":"null"},"StreamBufferSettings\":{"StreamBufferCount
\":"3","CtrlStreamBufferSizeInMB\":"5","StreamBufferSizeInMB\":"8"},"ErrorBehavior
\":{"FailOnNoTablesCaptured\":"true","ApplyErrorUpdatePolicy\":"LOG_ERROR","
"FailOnTransactionConsistencyBreached\":"false","RecoverableErrorThrottlingMax\":"1800,
"DataErrorEscalationPolicy\":"SUSPEND_TABLE","ApplyErrorEscalationCount\":"0,
"RecoverableErrorStopRetryAfterThrottlingMax\":"true","RecoverableErrorThrottling
\":"true","ApplyErrorFailOnTruncationDdl\":"false","DataTruncationErrorPolicy\":"
"LOG_ERROR","ApplyErrorInsertPolicy\":"LOG_ERROR","EventErrorPolicy\":"
"IGNORE","ApplyErrorEscalationPolicy\":"LOG_ERROR","RecoverableErrorCount
\":"-1","DataErrorEscalationCount\":"0","TableErrorEscalationPolicy\":"STOP_TASK
\","RecoverableErrorInterval\":"5","ApplyErrorDeletePolicy\":"IGNORE_RECORD",
"TableErrorEscalationCount\":"0","FullLoadIgnoreConflicts\":"true","DataErrorPolicy
\":"LOG_ERROR","TableErrorPolicy\":"SUSPEND_TABLE"},"TTSettings
\":{"TTS3Settings\":"null","TTRecordSettings\":"null","EnableTT\":"false"},
"FullLoadSettings\":{"CommitRate\":"10000","StopTaskCachedChangesApplied
\":"false","StopTaskCachedChangesNotApplied\":"false","MaxFullLoadSubTasks
\":"8","TransactionConsistencyTimeout\":"600","CreatePkAfterFullLoad\":"false,
"TargetTablePrepMode\":"DO_NOTHING"},"TargetMetadata\":{"ParallelApplyBufferSize
\":"0","ParallelApplyQueuesPerThread\":"0","ParallelApplyThreads\":"0","TargetSchema
\":"","InlineLobMaxSize\":"0","ParallelLoadQueuesPerThread\":"0","SupportLobs
\":"true","LobChunkSize\":"64","TaskRecoveryTableEnabled\":"false","ParallelLoadThreads
\":"0","LobMaxSize\":"0","BatchApplyEnabled\":"false","FullLobMode\":"true,
"LimitedSizeLobMode\":"false","LoadMaxFileSize\":"0","ParallelLoadBufferSize\":"0},
"BeforeImageSettings\":"null","ControlTablesSettings\":{"historyTimeslotInMinutes
\":"5","HistoryTimeslotInMinutes\":"5","StatusTableEnabled\":"false,
"SuspendedTablesTableEnabled\":"false","HistoryTableEnabled\":"false","ControlSchema
\":"","FullLoadExceptionTableEnabled\":"false"},"LoopbackPreventionSettings
\":"null","CharacterSetSettings\":"null","FailTaskWhenCleanTaskResourceFailed
\":"false","ChangeProcessingTuning\":{"StatementCacheSize\":"50","CommitTimeout
\":"1","BatchApplyPreserveTransaction\":"true","BatchApplyTimeoutMin\":"1,
"BatchSplitSize\":"0","BatchApplyTimeoutMax\":"30","MinTransactionSize\":"1000,
"MemoryKeepTime\":"60","BatchApplyMemoryLimit\":"500","MemoryLimitTotal\":"1024},

```



```
\ "ChangeProcessingDdlHandlingPolicy\": {\ "HandleSourceTableDropped\": true,
\ "HandleSourceTableTruncated\": true, \ "HandleSourceTableAltered\": true },
\ "PostProcessingRules\": null },
  \ "SourceEndpointArn\": "arn:aws:dms:us-
east-1:123456789012:endpoint:TZPWV2VCXEGHY0KVCRNHAKJ4Q3RUXACNGFGYWRI",
  \ "TableMappings\": {\ "rules\": [\ {\ "rule-type\": \ "selection\", \ "rule-id\":
\ "969761702\", \ "rule-name\": \ "969761702\", \ "object-locator\": {\ "schema-name\": \ "%table
\", \ "table-name\": \ "%example\", \ "rule-action\": \ "exclude\", \ "filters\": [\ ] } } ],
  \ "TargetEndpointArn\": "arn:aws:dms:us-
east-1:123456789012:endpoint:ABR8LB0QB3CZY33F7XV253NAJVBNPK6MJQVQVQA"
}
```

AwsDynamoDBRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für Ressourcen. `AwsDynamoDB`

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsDynamoDbTable

Das `AwsDynamoDbTable` Objekt enthält Details zu einer Amazon DynamoDB-Tabelle.

Im Folgenden finden Sie ein Beispiel für einen `AwsDynamoDbTable` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsDynamoDbTable` Attribute finden Sie [AwsDynamoDbTableDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsDynamoDbTable": {
  "AttributeDefinitions": [
    {
      "AttributeName": "attribute1",
      "AttributeType": "value 1"
    },
    {
      "AttributeName": "attribute2",
      "AttributeType": "value 2"
    },
    {
      "AttributeName": "attribute3",
      "AttributeType": "value 3"
    }
  ]
}
```

```

    }
  ],
  "BillingModeSummary": {
    "BillingMode": "PAY_PER_REQUEST",
    "LastUpdateToPayPerRequestDateTime": "2019-12-03T15:23:10.323Z"
  },
  "CreationDateTime": "2019-12-03T15:23:10.248Z",
  "DeletionProtectionEnabled": true,
  "GlobalSecondaryIndexes": [
    {
      "Backfilling": false,
      "IndexArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
index/exampleIndex",
      "IndexName": "standardsControlArnIndex",
      "IndexSizeBytes": 1862513,
      "IndexStatus": "ACTIVE",
      "ItemCount": 20,
      "KeySchema": [
        {
          "AttributeName": "City",
          "KeyType": "HASH"
        },
        {
          "AttributeName": "Date",
          "KeyType": "RANGE"
        }
      ],
      "Projection": {
        "NonKeyAttributes": ["predictorName"],
        "ProjectionType": "ALL"
      },
      "ProvisionedThroughput": {
        "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
        "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
        "NumberOfDecreasesToday": 0,
        "ReadCapacityUnits": 100,
        "WriteCapacityUnits": 50
      }
    },
  ],
  "GlobalTableVersion": "V1",
  "ItemCount": 2705,
  "KeySchema": [
    {

```

```

        "AttributeName": "zipcode",
        "KeyType": "HASH"
    }
],
"LatestStreamArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
stream/2019-12-03T23:23:10.248",
"LatestStreamLabel": "2019-12-03T23:23:10.248",
"LocalSecondaryIndexes": [
    {
        "IndexArn": "arn:aws:dynamodb:us-east-1:111122223333:table/exampleGroup/
index/exampleId",
        "IndexName": "CITY_DATE_INDEX_NAME",
        "KeySchema": [
            {
                "AttributeName": "zipcode",
                "KeyType": "HASH"
            }
        ],
        "Projection": {
            "NonKeyAttributes": ["predictorName"],
            "ProjectionType": "ALL"
        },
    }
],
"ProvisionedThroughput": {
    "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
    "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
    "NumberOfDecreasesToday": 0,
    "ReadCapacityUnits": 100,
    "WriteCapacityUnits": 50
},
"Replicas": [
    {
        "GlobalSecondaryIndexes":[
            {
                "IndexName": "CITY_DATE_INDEX_NAME",
                "ProvisionedThroughputOverride": {
                    "ReadCapacityUnits": 10
                }
            }
        ],
        "KmsMasterKeyId" : "KmsKeyId"
        "ProvisionedThroughputOverride": {
            "ReadCapacityUnits": 10
        }
    }
]

```

```

    },
    "RegionName": "regionName",
    "ReplicaStatus": "CREATING",
    "ReplicaStatusDescription": "replicaStatusDescription"
  }
],
"RestoreSummary" : {
  "SourceBackupArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
backup/backup1",
  "SourceTableArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable",
  "RestoreDateTime": "2020-06-22T17:40:12.322Z",
  "RestoreInProgress": true
},
"SseDescription": {
  "InaccessibleEncryptionDateTime": "2018-01-26T23:50:05.000Z",
  "Status": "ENABLED",
  "SseType": "KMS",
  "KmsMasterKeyArn": "arn:aws:kms:us-east-1:111122223333:key/key1"
},
"StreamSpecification" : {
  "StreamEnabled": true,
  "StreamViewType": "NEW_IMAGE"
},
"TableId": "example-table-id-1",
"TableName": "example-table",
"TableSizeBytes": 1862513,
"TableStatus": "ACTIVE"
}

```

AwsEc2Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für AwsEc2 Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter. [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsEc2ClientVpnEndpoint

Das AwsEc2ClientVpnEndpoint Objekt stellt Informationen über einen AWS Client VPN Endpunkt bereit. Ein Client-VPN-Endpunkt ist die Ressource, die Sie erstellen und konfigurieren, um Client-VPN-Sitzungen zu aktivieren und zu verwalten. Es handelt sich hier um den Beendigungspunkt für alle Client-VPN-Sitzungen.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2ClientVpnEndpoint` Objekt. Beschreibungen der `AwsEc2ClientVpnEndpoint` Attribute finden Sie unter [AwsEc2 ClientVpnEndpointDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2ClientVpnEndpoint": {
  "AuthenticationOptions": [
    {
      "MutualAuthentication": {
        "ClientRootCertificateChainArn": "arn:aws:acm:us-east-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
      },
      "Type": "certificate-authentication"
    }
  ],
  "ClientCidrBlock": "10.0.0.0/22",
  "ClientConnectOptions": {
    "Enabled": false
  },
  "ClientLoginBannerOptions": {
    "Enabled": false
  },
  "ClientVpnEndpointId": "cvpn-endpoint-00c5d11fc4729f2a5",
  "ConnectionLogOptions": {
    "Enabled": false
  },
  "Description": "test",
  "DnsServer": ["10.0.0.0"],
  "ServerCertificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "SecurityGroupIdSet": [
    "sg-0f7a177b82b443691"
  ],
  "SelfServicePortalUrl": "https://self-service.clientvpn.amazonaws.com/endpoints/cvpn-endpoint-00c5d11fc4729f2a5",
  "SessionTimeoutHours": 24,
  "SplitTunnel": false,
  "TransportProtocol": "udp",
  "VpcId": "vpc-1a2b3c4d5e6f1a2b3",
  "VpnPort": 443
}
```

AwsEc2Eip

Das AwsEc2Eip Objekt stellt Informationen über eine Elastic IP-Adresse bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das AwsEc2Eip Objekt. Beschreibungen der AwsEc2Eip Attribute finden Sie unter [AwsEc2 EipDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2Eip": {
  "InstanceId": "instance1",
  "PublicIp": "192.0.2.04",
  "AllocationId": "eipalloc-example-id-1",
  "AssociationId": "eipassoc-example-id-1",
  "Domain": "vpc",
  "PublicIpv4Pool": "anycompany",
  "NetworkBorderGroup": "eu-central-1",
  "NetworkInterfaceId": "eni-example-id-1",
  "NetworkInterfaceOwnerId": "777788889999",
  "PrivateIpAddress": "192.0.2.03"
}
```

AwsEc2Instance

Das AwsEc2Instance Objekt enthält Details zu einer EC2 Amazon-Instance.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das AwsEc2Instance Objekt. Beschreibungen der AwsEc2Instance Attribute finden Sie unter [AwsEc2 InstanceDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2Instance": {
  "IamInstanceProfileArn": "arn:aws:iam::123456789012:instance-profile/AdminRole",
  "ImageId": "ami-1234",
  "IPv4Addresses": [ "1.1.1.1" ],
  "IPv6Addresses": [ "2001:db8:1234:1a2b::123" ],
  "KeyName": "my_keypair",
  "LaunchedAt": "2018-05-08T16:46:19.000Z",
  "MetadataOptions": {
```

```

    "HttpEndpoint": "enabled",
    "HttpProtocolIpv6": "enabled",
    "HttpPutResponseHopLimit": 1,
    "HttpTokens": "optional",
    "InstanceMetadataTags": "disabled",
  },
  "Monitoring": {
    "State": "disabled"
  },
  "NetworkInterfaces": [
    {
      "NetworkInterfaceId": "eni-e5aa89a3"
    }
  ],
  "SubnetId": "subnet-123",
  "Type": "i3.xlarge",
  "VpcId": "vpc-123"
}

```

AwsEc2LaunchTemplate

Das `AwsEc2LaunchTemplate` Objekt enthält Details zu einer Amazon Elastic Compute Cloud-Startvorlage, die Informationen zur Instance-Konfiguration spezifiziert.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2LaunchTemplate` Objekt. Beschreibungen der `AwsEc2LaunchTemplate` Attribute finden Sie unter [AwsEc2 LaunchTemplateDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsEc2LaunchTemplate": {
  "DefaultVersionNumber": "1",
  "ElasticGpuSpecifications": ["string"],
  "ElasticInferenceAccelerators": ["string"],
  "Id": "lt-0a16e9802800bdd85",
  "ImageId": "ami-0d5eff06f840b45e9",
  "LatestVersionNumber": "1",
  "LaunchTemplateData": {
    "BlockDeviceMappings": [{
      "DeviceName": "/dev/xvda",
      "Ebs": {
        "DeleteonTermination": true,
        "Encrypted": true,

```

```

    "SnapshotId": "snap-01047646ec075f543",
    "VolumeSize": 8,
    "VolumeType": "gp2"
  }
}],
"MetadataOptions": {
  "HttpTokens": "enabled",
  "HttpPutResponseHopLimit": 1
},
"Monitoring": {
  "Enabled": true,
  "NetworkInterfaces": [{
    "AssociatePublicIpAddress": true,
  }],
"LaunchTemplateName": "string",
"LicenseSpecifications": ["string"],
"SecurityGroupIds": ["sg-01fce87ad6e019725"],
"SecurityGroups": ["string"],
"TagSpecifications": ["string"]
}

```

AwsEc2NetworkAcl

Das `AwsEc2NetworkAcl` Objekt enthält Details zu einer Amazon EC2 Network Access Control List (ACL).

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2NetworkAcl` Objekt. Beschreibungen der `AwsEc2NetworkAcl` Attribute finden Sie unter [AwsEc2NetworkAclDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsEc2NetworkAcl": {
  "IsDefault": false,
  "NetworkAclId": "acl-1234567890abcdef0",
  "OwnerId": "123456789012",
  "VpcId": "vpc-1234abcd",
  "Associations": [{
    "NetworkAclAssociationId": "aclassoc-abcd1234",
    "NetworkAclId": "acl-021345abcdef6789",
    "SubnetId": "subnet-abcd1234"
  }],
  "Entries": [{

```



```

    "CidrBlock": "10.24.34.0/23",
    "Egress": true,
    "IcmpTypeCode": {
      "Code": 10,
      "Type": 30
    },
    "Ipv6CidrBlock": "2001:DB8::/32",
    "PortRange": {
      "From": 20,
      "To": 40
    },
    "Protocol": "tcp",
    "RuleAction": "allow",
    "RuleNumber": 100
  }]
}
```

AwsEc2NetworkInterface

Das `AwsEc2NetworkInterface` Objekt stellt Informationen über eine EC2 Amazon-Netzwerkschnittstelle bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2NetworkInterface` Objekt. Beschreibungen der `AwsEc2NetworkInterface` Attribute finden Sie unter [AwsEc2 NetworkInterfaceDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsEc2NetworkInterface": {
  "Attachment": {
    "AttachTime": "2019-01-01T03:03:21Z",
    "AttachmentId": "eni-attach-43348162",
    "DeleteOnTermination": true,
    "DeviceIndex": 123,
    "InstanceId": "i-1234567890abcdef0",
    "InstanceOwnerId": "123456789012",
    "Status": 'ATTACHED'
  },
  "SecurityGroups": [
    {
      "GroupName": "my-security-group",
      "GroupId": "sg-903004f8"
    },
  ],
}
```

```

],
"NetworkInterfaceId": 'eni-686ea200',
"SourceDestCheck": false
}

```

AwsEc2RouteTable

Das `AwsEc2RouteTable` Objekt stellt Informationen über eine EC2 Amazon-Routentabelle bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2RouteTable` Objekt. Beschreibungen der `AwsEc2RouteTable` Attribute finden Sie unter [AwsEc2RouteTableDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsEc2RouteTable": {
  "AssociationSet": [{
    "AssociationSet": {
      "State": "associated"
    },
    "Main": true,
    "RouteTableAssociationId": "rtbassoc-08e706c45de9f7512",
    "RouteTableId": "rtb-0a59bde9cf2548e34",
  }],
  "PropogatingVgwSet": [],
  "RouteTableId": "rtb-0a59bde9cf2548e34",
  "RouteSet": [
    {
      "DestinationCidrBlock": "10.24.34.0/23",
      "GatewayId": "local",
      "Origin": "CreateRouteTable",
      "State": "active"
    },
    {
      "DestinationCidrBlock": "10.24.34.0/24",
      "GatewayId": "igw-0242c2d7d513fc5d3",
      "Origin": "CreateRoute",
      "State": "active"
    }
  ],
  "VpcId": "vpc-0c250a5c33f51d456"
}

```

AwsEc2SecurityGroup

Das `AwsEc2SecurityGroup` Objekt beschreibt eine EC2 Amazon-Sicherheitsgruppe.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2SecurityGroup` Objekt. Beschreibungen der `AwsEc2SecurityGroup` Attribute finden Sie unter [AwsEc2 SecurityGroupDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2SecurityGroup": {
  "GroupName": "MySecurityGroup",
  "GroupId": "sg-903004f8",
  "OwnerId": "123456789012",
  "VpcId": "vpc-1a2b3c4d",
  "IpPermissions": [
    {
      "IpProtocol": "-1",
      "IpRanges": [],
      "UserIdGroupPairs": [
        {
          "UserId": "123456789012",
          "GroupId": "sg-903004f8"
        }
      ],
      "PrefixListIds": [
        {"PrefixListId": "pl-63a5400a"}
      ]
    },
    {
      "PrefixListIds": [],
      "FromPort": 22,
      "IpRanges": [
        {
          "CidrIp": "203.0.113.0/24"
        }
      ],
      "ToPort": 22,
      "IpProtocol": "tcp",
      "UserIdGroupPairs": []
    }
  ]
}
```

AwsEc2Subnet

Das `AwsEc2Subnet` Objekt stellt Informationen über ein Subnetz in Amazon EC2 bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2Subnet` Objekt. Beschreibungen der `AwsEc2Subnet` Attribute finden Sie unter [AwsEc2 SubnetDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
AwsEc2Subnet: {
  "AssignIpv6AddressOnCreation": false,
  "AvailabilityZone": "us-west-2c",
  "AvailabilityZoneId": "usw2-az3",
  "AvailableIpAddressCount": 8185,
  "CidrBlock": "10.0.0.0/24",
  "DefaultForAz": false,
  "MapPublicIpOnLaunch": false,
  "OwnerId": "123456789012",
  "State": "available",
  "SubnetArn": "arn:aws:ec2:us-west-2:123456789012:subnet/subnet-d5436c93",
  "SubnetId": "subnet-d5436c93",
  "VpcId": "vpc-153ade70",
  "Ipv6CidrBlockAssociationSet": [{
    "AssociationId": "subnet-cidr-assoc-EXAMPLE",
    "Ipv6CidrBlock": "2001:DB8::/32",
    "CidrBlockState": "associated"
  }]
}
```

AwsEc2TransitGateway

Das `AwsEc2TransitGateway` Objekt enthält Details zu einem Amazon EC2 Transit Gateway, das Ihre virtuellen privaten Clouds (VPCs) und lokalen Netzwerke miteinander verbindet.

Im Folgenden finden Sie ein Beispiel für einen `AwsEc2TransitGateway` Befund im AWS Security Finding Format (ASFF). Beschreibungen von `AwsEc2TransitGateway` Attributen finden Sie unter [AwsEc2 TransitGatewayDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2TransitGateway": {
```

```

"AmazonSideAsn": 65000,
"AssociationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
"AutoAcceptSharedAttachments": "disable",
"DefaultRouteTableAssociation": "enable",
"DefaultRouteTablePropagation": "enable",
"Description": "sample transit gateway",
"DnsSupport": "enable",
"Id": "tgw-042ae6bf7a5c126c3",
"MulticastSupport": "disable",
"PropagationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
"TransitGatewayCidrBlocks": ["10.0.0.0/16"],
"VpnEcmpSupport": "enable"
}

```

AwsEc2Volume

Das `AwsEc2Volume` Objekt enthält Details zu einem EC2 Amazon-Volume.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2Volume` Objekt. Beschreibungen der `AwsEc2Volume` Attribute finden Sie unter [AwsEc2 VolumeDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsEc2Volume": {
  "Attachments": [
    {
      "AttachTime": "2017-10-17T14:47:11Z",
      "DeleteOnTermination": true,
      "InstanceId": "i-123abc456def789g",
      "Status": "attached"
    }
  ],
  "CreateTime": "2020-02-24T15:54:30Z",
  "Encrypted": true,
  "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
  "Size": 80,
  "SnapshotId": "",
  "Status": "available"
}

```

AwsEc2Vpc

Das AwsEc2Vpc Objekt enthält Details zu einer EC2 Amazon-VPC.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das AwsEc2Vpc Objekt. Beschreibungen der AwsEc2Vpc Attribute finden Sie unter [AwsEc2 VpcDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2Vpc": {
  "CidrBlockAssociationSet": [
    {
      "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
      "CidrBlock": "192.0.2.0/24",
      "CidrBlockState": "associated"
    }
  ],
  "DhcpOptionsId": "dopt-4e42ce28",
  "Ipv6CidrBlockAssociationSet": [
    {
      "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
      "CidrBlockState": "associated",
      "Ipv6CidrBlock": "192.0.2.0/24"
    }
  ],
  "State": "available"
}
```

AwsEc2VpcEndpointService

Das AwsEc2VpcEndpointService Objekt enthält Details zur Dienstkonfiguration für einen VPC-Endpunktdienst.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das AwsEc2VpcEndpointService Objekt. Beschreibungen der AwsEc2VpcEndpointService Attribute finden Sie unter [AwsEc2 VpcEndpointServiceDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2VpcEndpointService": {
```

```

    "ServiceType": [
      {
        "ServiceType": "Interface"
      }
    ],
    "ServiceId": "vpce-svc-example1",
    "ServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example1",
    "ServiceState": "Available",
    "AvailabilityZones": [
      "us-east-1"
    ],
    "AcceptanceRequired": true,
    "ManagesVpcEndpoints": false,
    "NetworkLoadBalancerArns": [
      "arn:aws:elasticloadbalancing:us-east-1:444455556666:loadbalancer/net/my-network-load-balancer/example1"
    ],
    "GatewayLoadBalancerArns": [],
    "BaseEndpointDnsNames": [
      "vpce-svc-04eec859668b51c34.us-east-1.vpce.amazonaws.com"
    ],
    "PrivateDnsName": "my-private-dns"
  }

```

AwsEc2VpcPeeringConnection

Das `AwsEc2VpcPeeringConnection` Objekt enthält Details zur Netzwerkverbindung zwischen zwei VPCs Objekten.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2VpcPeeringConnection` Objekt. Beschreibungen der `AwsEc2VpcPeeringConnection` Attribute finden Sie unter [AwsEc2 VpcPeeringConnectionDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsEc2VpcPeeringConnection": {
  "AcceptorVpcInfo": {
    "CidrBlock": "10.0.0.0/28",
    "CidrBlockSet": [{
      "CidrBlock": "10.0.0.0/28"
    }],
    "Ipv6CidrBlockSet": [{

```

```

    "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
  }],
  "OwnerId": "012345678910",
  "PeeringOptions": {
    "AllowDnsResolutionFromRemoteVpc": true,
    "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
    "AllowEgressFromLocalVpcToRemoteClassicLink": true
  },
  "Region": "us-west-2",
  "VpcId": "vpc-i123456"
},
"ExpirationTime": "2022-02-18T15:31:53.161Z",
"RequesterVpcInfo": {
  "CidrBlock": "192.168.0.0/28",
  "CidrBlockSet": [{
    "CidrBlock": "192.168.0.0/28"
  }],
  "Ipv6CidrBlockSet": [{
    "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
  }],
  "OwnerId": "012345678910",
  "PeeringOptions": {
    "AllowDnsResolutionFromRemoteVpc": true,
    "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
    "AllowEgressFromLocalVpcToRemoteClassicLink": true
  },
  "Region": "us-west-2",
  "VpcId": "vpc-i123456"
},
"Status": {
  "Code": "initiating-request",
  "Message": "Active"
},
"VpcPeeringConnectionId": "pcx-1a2b3c4d"
}

```

AwsEcrRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für AwsEcr Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter. [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsEcrContainerImage

Das `AwsEcrContainerImage` Objekt stellt Informationen zu einem Amazon ECR-Bild bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEcrContainerImage` Objekt. Beschreibungen der `AwsEcrContainerImage` Attribute finden Sie [AwsEcrContainerImageDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEcrContainerImage": {
  "RegistryId": "123456789012",
  "RepositoryName": "repository-name",
  "Architecture": "amd64"
  "ImageDigest":
    "sha256:a568e5c7a953fbeaa2904ac83401f93e4a076972dc1bae527832f5349cd2fb10",
  "ImageTags": ["00000000-0000-0000-0000-000000000000"],
  "ImagePublishedAt": "2019-10-01T20:06:12Z"
}
```

AwsEcrRepository

Das `AwsEcrRepository` Objekt stellt Informationen über ein Amazon Elastic Container Registry-Repository bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEcrRepository` Objekt. Beschreibungen der `AwsEcrRepository` Attribute finden Sie [AwsEcrRepositoryDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEcrRepository": {
  "LifecyclePolicy": {
    "RegistryId": "123456789012",
  },
  "RepositoryName": "sample-repo",
  "Arn": "arn:aws:ecr:us-west-2:111122223333:repository/sample-repo",
  "ImageScanningConfiguration": {
    "ScanOnPush": true
  },
  "ImageTagMutability": "IMMUTABLE"
}
```

AwsEcsRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsEcs` Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsEcsCluster

Das `AwsEcsCluster` Objekt enthält Details zu einem Amazon Elastic Container Service-Cluster.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEcsCluster` Objekt. Beschreibungen der `AwsEcsCluster` Attribute finden Sie [AwsEcsClusterDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEcsCluster": {
  "CapacityProviders": [],
  "ClusterSettings": [
    {
      "Name": "containerInsights",
      "Value": "enabled"
    }
  ],
  "Configuration": {
    "ExecuteCommandConfiguration": {
      "KmsKeyId": "kmsKeyId",
      "LogConfiguration": {
        "CloudWatchEncryptionEnabled": true,
        "CloudWatchLogGroupName": "cloudWatchLogGroupName",
        "S3BucketName": "s3BucketName",
        "S3EncryptionEnabled": true,
        "S3KeyPrefix": "s3KeyPrefix"
      },
      "Logging": "DEFAULT"
    },
    "DefaultCapacityProviderStrategy": [
      {
        "Base": 0,
        "CapacityProvider": "capacityProvider",
```

```

    "Weight": 1
  }
]
}

```

AwsEcsContainer

Das `AwsEcsContainer` Objekt enthält Details zu einem Amazon ECS-Container.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEcsContainer` Objekt. Beschreibungen der `AwsEcsContainer` Attribute finden Sie [AwsEcsContainerDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsEcsContainer": {
  "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
  "MountPoints": [{
    "ContainerPath": "/mnt/etc",
    "SourceVolume": "vol-03909e9"
  }],
  "Name": "knote",
  "Privileged": true
}

```

AwsEcsService

Das `AwsEcsService` Objekt bietet Details zu einem Service innerhalb eines Amazon ECS-Clusters.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEcsService` Objekt. Beschreibungen der `AwsEcsService` Attribute finden Sie [AwsEcsServiceDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsEcsService": {
  "CapacityProviderStrategy": [
    {
      "Base": 12,
      "CapacityProvider": "",
      "Weight": ""
    }
  ]
}

```

```
],
"Cluster": "arn:aws:ecs:us-east-1:111122223333:cluster/example-ecs-cluster",
"DeploymentConfiguration": {
  "DeploymentCircuitBreaker": {
    "Enable": false,
    "Rollback": false
  },
  "MaximumPercent": 200,
  "MinimumHealthyPercent": 100
},
"DeploymentController": "",
"DesiredCount": 1,
"EnableEcsManagedTags": false,
"EnableExecuteCommand": false,
"HealthCheckGracePeriodSeconds": 1,
"LaunchType": "FARGATE",
"LoadBalancers": [
  {
    "ContainerName": "",
    "ContainerPort": 23,
    "LoadBalancerName": "",
    "TargetGroupArn": ""
  }
],
"Name": "sample-app-service",
"NetworkConfiguration": {
  "AwsVpcConfiguration": {
    "Subnets": [
      "Subnet-example1",
      "Subnet-example2"
    ],
    "SecurityGroups": [
      "Sg-0ce48e9a6e5b457f5"
    ],
    "AssignPublicIp": "ENABLED"
  }
},
"PlacementConstraints": [
  {
    "Expression": "",
    "Type": ""
  }
],
"PlacementStrategies": [
```

```

    {
        "Field": "",
        "Type": ""
    }
],
"PlatformVersion": "LATEST",
"PropagateTags": "",
"Role": "arn:aws:iam::111122223333:role/aws-servicerole/ecs.amazonaws.com/ServiceRoleForECS",
"SchedulingStrategy": "REPLICA",
"ServiceName": "sample-app-service",
"ServiceArn": "arn:aws:ecs:us-east-1:111122223333:service/example-ecs-cluster/sample-app-service",
"ServiceRegistries": [
    {
        "ContainerName": "",
        "ContainerPort": 1212,
        "Port": 1221,
        "RegistryArn": ""
    }
],
"TaskDefinition": "arn:aws:ecs:us-east-1:111122223333:task-definition/example-taskdef:1"
}

```

AwsEcsTask

Das `AwsEcsTask` Objekt enthält Details zu einer Amazon ECS-Aufgabe.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEcsTask` Objekt. Beschreibungen der `AwsEcsTask` Attribute finden Sie [AwsEcsTask](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsEcsTask": {
    "ClusterArn": "arn:aws:ecs:us-west-2:123456789012:task/MyCluster/1234567890123456789",
    "CreatedAt": "1557134011644",
    "Group": "service:fargate-service",
    "StartedAt": "1557134011644",
    "StartedBy": "ecs-svc/1234567890123456789",
    "TaskDefinitionArn": "arn:aws:ecs:us-west-2:123456789012:task-definition/sample-fargate:2",

```

```

"Version": 3,
"Volumes": [{
  "Name": "string",
  "Host": {
    "SourcePath": "string"
  }
}],
"Containers": {
  "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
  "MountPoints": [{
    "ContainerPath": "/mnt/etc",
    "SourceVolume": "vol-03909e9"
  }],
  "Name": "knote",
  "Privileged": true
}
}

```

AwsEcsTaskDefinition

Das `AwsEcsTaskDefinition` Objekt enthält Details zu einer Aufgabendefinition. Eine Aufgabendefinition beschreibt die Container- und Volume-Definitionen einer Amazon Elastic Container Service-Aufgabe.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEcsTaskDefinition` Objekt. Beschreibungen der `AwsEcsTaskDefinition` Attribute finden Sie [AWS EcsTaskDefinitionDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsEcsTaskDefinition": {
  "ContainerDefinitions": [
    {
      "Command": ['ruby', 'hi.rb'],
      "Cpu": 128,
      "Essential": true,
      "HealthCheck": {
        "Command": ["CMD-SHELL", "curl -f http://localhost/ || exit 1"],
        "Interval": 10,
        "Retries": 3,
        "StartPeriod": 5,
        "Timeout": 20
      }
    }
  ]
}

```

```

    },
    "Image": "tongueroo/sinatra:latest",
    "Interactive": true,
    "Links": [],
    "LogConfiguration": {
      "LogDriver": "awslogs",
      "Options": {
        "awslogs-group": "/ecs/sinatra-hi",
        "awslogs-region": "ap-southeast-1",
        "awslogs-stream-prefix": "ecs"
      },
      "SecretOptions": []
    },
    "MemoryReservation": 128,
    "Name": "web",
    "PortMappings": [
      {
        "ContainerPort": 4567,
        "HostPort": 4567,
        "Protocol": "tcp"
      }
    ],
    "Privileged": true,
    "StartTimeout": 10,
    "StopTimeout": 100,
  }
],
"Family": "sinatra-hi",
"NetworkMode": "host",
"RequiresCompatibilities": ["EC2"],
"Status": "ACTIVE",
"TaskRoleArn": "arn:aws:iam::111122223333:role/ecsTaskExecutionRole",
}

```

AwsEfsRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für AwsEfs Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter. [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsEfsAccessPoint

Das `AwsEfsAccessPoint` Objekt enthält Details zu Dateien, die im Amazon Elastic File System gespeichert sind.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEfsAccessPoint` Objekt. Beschreibungen der `AwsEfsAccessPoint` Attribute finden Sie [AwsEfsAccessPointDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEfsAccessPoint": {
  "AccessPointId": "fsap-05c4c0e79ba0b118a",
  "Arn": "arn:aws:elasticfilesystem:us-east-1:863155670886:access-point/
fsap-05c4c0e79ba0b118a",
  "ClientToken": "AccessPointCompliant-ASk06ZZSXsEp",
  "FileSystemId": "fs-0f8137f731cb32146",
  "PosixUser": {
    "Gid": "1000",
    "SecondaryGids": ["0", "4294967295"],
    "Uid": "1234"
  },
  "RootDirectory": {
    "CreationInfo": {
      "OwnerGid": "1000",
      "OwnerUid": "1234",
      "Permissions": "777"
    },
    "Path": "/tmp/example"
  }
}
```

AwsEksRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsEks` Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsEksCluster

Das `AwsEksCluster` Objekt enthält Details zu einem Amazon EKS-Cluster.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEksCluster` Objekt. Beschreibungen der `AwsEksCluster` Attribute finden Sie [AwsEksClusterDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
{
  "AwsEksCluster": {
    "Name": "example",
    "Arn": "arn:aws:eks:us-west-2:222222222222:cluster/example",
    "CreatedAt": 1565804921.901,
    "Version": "1.12",
    "RoleArn": "arn:aws:iam::222222222222:role/example-cluster-ServiceRole-1XWBQWYSFRE2Q",
    "ResourcesVpcConfig": {
      "EndpointPublicAccess": false,
      "SubnetIds": [
        "subnet-021345abcdef6789",
        "subnet-abcdef01234567890",
        "subnet-1234567890abcdef0"
      ],
      "SecurityGroupIds": [
        "sg-abcdef01234567890"
      ]
    },
    "Logging": {
      "ClusterLogging": [
        {
          "Types": [
            "api",
            "audit",
            "authenticator",
            "controllerManager",
            "scheduler"
          ],
          "Enabled": true
        }
      ]
    },
    "Status": "CREATING",
    "CertificateAuthorityData": {},
  }
}
```

AwsElasticBeanstalkRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für Ressourcen. `AwsElasticBeanstalk`

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter. [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsElasticBeanstalkEnvironment

Das `AwsElasticBeanstalkEnvironment` Objekt enthält Details zu einer AWS Elastic Beanstalk Umgebung.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsElasticBeanstalkEnvironment` Objekt. Beschreibungen der `AwsElasticBeanstalkEnvironment` Attribute finden Sie [AwsElasticBeanstalkEnvironmentDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsElasticBeanstalkEnvironment": {
  "ApplicationName": "MyApplication",
  "Cname": "myexampleapp-env.devo-2.elasticbeanstalk-internal.com",
  "DateCreated": "2021-04-30T01:38:01.090Z",
  "DateUpdated": "2021-04-30T01:38:01.090Z",
  "Description": "Example description of my awesome application",
  "EndpointUrl": "eb-dv-e-p-AWSEBLoa-abcdef01234567890-021345abcdef6789.us-east-1.elb.amazonaws.com",
  "EnvironmentArn": "arn:aws:elasticbeanstalk:us-east-1:123456789012:environment/MyApplication/myapplication-env",
  "EnvironmentId": "e-abcd1234",
  "EnvironmentLinks": [
    {
      "EnvironmentName": "myexampleapp-env",
      "LinkName": "myapplicationLink"
    }
  ],
  "EnvironmentName": "myapplication-env",
  "OptionSettings": [
    {
      "Namespace": "aws:elasticbeanstalk:command",
      "OptionName": "BatchSize",
```

```

        "Value": "100"
      },
      {
        "Namespace": "aws:elasticbeanstalk:command",
        "OptionName": "Timeout",
        "Value": "600"
      },
      {
        "Namespace": "aws:elasticbeanstalk:command",
        "OptionName": "BatchSizeType",
        "Value": "Percentage"
      },
      {
        "Namespace": "aws:elasticbeanstalk:command",
        "OptionName": "IgnoreHealthCheck",
        "Value": "false"
      },
      {
        "Namespace": "aws:elasticbeanstalk:application",
        "OptionName": "Application Healthcheck URL",
        "Value": "TCP:80"
      }
    ],
    "PlatformArn": "arn:aws:elasticbeanstalk:us-east-1::platform/Tomcat 8 with Java 8
running on 64bit Amazon Linux/2.7.7",
    "SolutionStackName": "64bit Amazon Linux 2017.09 v2.7.7 running Tomcat 8 Java 8",
    "Status": "Ready",
    "Tier": {
      "Name": "WebServer"
      "Type": "Standard"
      "Version": "1.0"
    },
    "VersionLabel": "Sample Application"
  }
}

```

AwsElasticSearchRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für AwsElasticSearch Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter. [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsElasticSearchDomain

Das `AwsElasticSearchDomain` Objekt enthält Details zu einer Amazon OpenSearch Service-Domain.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsElasticSearchDomain` Objekt. Beschreibungen der `AwsElasticSearchDomain` Attribute finden Sie [AwsElasticSearchDomainDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsElasticSearchDomain": {
  "AccessPolicies": "string",
  "DomainStatus": {
    "DomainId": "string",
    "DomainName": "string",
    "Endpoint": "string",
    "Endpoints": {
      "string": "string"
    }
  },
  "DomainEndpointOptions": {
    "EnforceHTTPS": boolean,
    "TLSSecurityPolicy": "string"
  },
  "ElasticsearchClusterConfig": {
    "DedicatedMasterCount": number,
    "DedicatedMasterEnabled": boolean,
    "DedicatedMasterType": "string",
    "InstanceCount": number,
    "InstanceType": "string",
    "ZoneAwarenessConfig": {
      "AvailabilityZoneCount": number
    },
    "ZoneAwarenessEnabled": boolean
  },
  "ElasticsearchVersion": "string",
  "EncryptionAtRestOptions": {
    "Enabled": boolean,
    "KmsKeyId": "string"
  },
  "LogPublishingOptions": {
    "AuditLogs": {
```

```

        "CloudWatchLogsLogGroupArn": "string",
        "Enabled": boolean
    },
    "IndexSlowLogs": {
        "CloudWatchLogsLogGroupArn": "string",
        "Enabled": boolean
    },
    "SearchSlowLogs": {
        "CloudWatchLogsLogGroupArn": "string",
        "Enabled": boolean
    }
},
"NodeToNodeEncryptionOptions": {
    "Enabled": boolean
},
"ServiceSoftwareOptions": {
    "AutomatedUpdateDate": "string",
    "Cancellable": boolean,
    "CurrentVersion": "string",
    "Description": "string",
    "NewVersion": "string",
    "UpdateAvailable": boolean,
    "UpdateStatus": "string"
},
"VPCOptions": {
    "AvailabilityZones": [
        "string"
    ],
    "SecurityGroupIds": [
        "string"
    ],
    "SubnetIds": [
        "string"
    ],
    "VPCId": "string"
}
}

```

AwsElbRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für AwsElb Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsElbLoadBalancer

Das `AwsElbLoadBalancer` Objekt enthält Details zu einem Classic Load Balancer.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsElbLoadBalancer` Objekt. Beschreibungen der `AwsElbLoadBalancer` Attribute finden Sie [AwsElbLoadBalancerDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsElbLoadBalancer": {
  "AvailabilityZones": ["us-west-2a"],
  "BackendServerDescriptions": [
    {
      "InstancePort": 80,
      "PolicyNames": ["doc-example-policy"]
    }
  ],
  "CanonicalHostedZoneName": "Z3DZXE0EXAMPLE",
  "CanonicalHostedZoneNameID": "my-load-balancer-444455556666.us-
west-2.elb.amazonaws.com",
  "CreatedTime": "2020-08-03T19:22:44.637Z",
  "DnsName": "my-load-balancer-444455556666.us-west-2.elb.amazonaws.com",
  "HealthCheck": {
    "HealthyThreshold": 2,
    "Interval": 30,
    "Target": "HTTP:80/png",
    "Timeout": 3,
    "UnhealthyThreshold": 2
  },
  "Instances": [
    {
      "InstanceId": "i-example"
    }
  ],
  "ListenerDescriptions": [
    {
      "Listener": {
        "InstancePort": 443,
        "InstanceProtocol": "HTTPS",
        "LoadBalancerPort": 443,
```

```

        "Protocol": "HTTPS",
        "SslCertificateId": "arn:aws:iam::444455556666:server-certificate/my-
server-cert"
    },
    "PolicyNames": ["ELBSecurityPolicy-TLS-1-2-2017-01"]
}
],
"LoadBalancerAttributes": {
    "AccessLog": {
        "EmitInterval": 60,
        "Enabled": true,
        "S3BucketName": "amzn-s3-demo-bucket",
        "S3BucketPrefix": "doc-example-prefix"
    },
    "ConnectionDraining": {
        "Enabled": false,
        "Timeout": 300
    },
    "ConnectionSettings": {
        "IdleTimeout": 30
    },
    "CrossZoneLoadBalancing": {
        "Enabled": true
    },
    "AdditionalAttributes": [{
        "Key": "elb.http.desyncmitigationmode",
        "Value": "strictest"
    }]
},
"LoadBalancerName": "example-load-balancer",
"Policies": {
    "AppCookieStickinessPolicies": [
        {
            "CookieName": "",
            "PolicyName": ""
        }
    ],
    "LbCookieStickinessPolicies": [
        {
            "CookieExpirationPeriod": 60,
            "PolicyName": "my-example-cookie-policy"
        }
    ]
},

```

```

    "OtherPolicies": [
      "my-PublicKey-policy",
      "my-authentication-policy",
      "my-SSLNegotiation-policy",
      "my-ProxyProtocol-policy",
      "ELBSecurityPolicy-2015-03"
    ],
    "Scheme": "internet-facing",
    "SecurityGroups": ["sg-example"],
    "SourceSecurityGroup": {
      "GroupName": "my-elb-example-group",
      "OwnerAlias": "444455556666"
    },
    "Subnets": ["subnet-example"],
    "VpcId": "vpc-a01106c2"
  }
}

```

AwsElbv2LoadBalancer

Das Objekt `AwsElbv2LoadBalancer` stellt Informationen über einen Load Balancer bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsElbv2LoadBalancer` Objekt. Beschreibungen der `AwsElbv2LoadBalancer` Attribute finden Sie unter [AwsElbv2 LoadBalancerDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsElbv2LoadBalancer": {
  "AvailabilityZones": {
    "SubnetId": "string",
    "ZoneName": "string"
  },
  "CanonicalHostedZoneId": "string",
  "CreatedTime": "string",
  "DNSName": "string",
  "IpAddressType": "string",
  "LoadBalancerAttributes": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],

```



```
    "Scheme": "string",
    "SecurityGroups": [ "string" ],
    "State": {
        "Code": "string",
        "Reason": "string"
    },
    "Type": "string",
    "VpcId": "string"
}
```

AwsEventBridgeRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für AwsEventBridge Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter. [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsEventSchemasRegistry

Das AwsEventSchemasRegistry Objekt stellt Informationen über eine EventBridge Amazon-Schemaregistrierung bereit. Ein Schema definiert die Struktur der Ereignisse, an die gesendet werden EventBridge. Schemaregister sind Container, die Ihre Schemas sammeln und logisch gruppieren.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt.

AwsEventSchemasRegistry Beschreibungen der AwsEventSchemasRegistry Attribute finden Sie [AwsEventSchemasRegistry](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEventSchemasRegistry": {
    "Description": "This is an example event schema registry.",
    "RegistryArn": "arn:aws:schemas:us-east-1:123456789012:registry/schema-registry",
    "RegistryName": "schema-registry"
}
```

AwsEventsEndpoint

Das AwsEventsEndpoint Objekt stellt Informationen über einen EventBridge globalen Amazon-Endpunkt bereit. Der Endpunkt kann die Verfügbarkeit Ihrer Anwendung verbessern, indem er sie regional fehlertolerant macht.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt. `AwsEventsEndpoint` Beschreibungen der `AwsEventsEndpoint` Attribute finden Sie [AWSEventsEndpointDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEventsEndpoint": {
  "Arn": "arn:aws:events:us-east-1:123456789012:endpoint/my-endpoint",
  "Description": "This is a sample endpoint.",
  "EndpointId": "04k1exajoy.veo",
  "EndpointUrl": "https://04k1exajoy.veo.endpoint.events.amazonaws.com",
  "EventBuses": [
    {
      "EventBusArn": "arn:aws:events:us-east-1:123456789012:event-bus/default"
    },
    {
      "EventBusArn": "arn:aws:events:us-east-2:123456789012:event-bus/default"
    }
  ],
  "Name": "my-endpoint",
  "ReplicationConfig": {
    "State": "ENABLED"
  },
  "RoleArn": "arn:aws:iam::123456789012:role/service-role/Amazon_EventBridge_Invoke_Event_Bus_1258925394",
  "RoutingConfig": {
    "FailoverConfig": {
      "Primary": {
        "HealthCheck": "arn:aws:route53:::healthcheck/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
      },
      "Secondary": {
        "Route": "us-east-2"
      }
    }
  },
  "State": "ACTIVE"
}
```

AwsEventsEventbus

Das `AwsEventsEventbus` Objekt stellt Informationen über einen EventBridge globalen Amazon-Endpoint bereit. Der Endpoint kann die Verfügbarkeit Ihrer Anwendung verbessern, indem er sie regional fehlertolerant macht.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt. `AwsEventsEventbus` Beschreibungen der `AwsEventsEventbus` Attribute finden Sie [AWSEventsEventbusDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEventsEventbus":
  "Arn": "arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus",
  "Name": "my-event-bus",
  "Policy": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement\": [\n    {\n      \"Sid\":\n      \"AllowAllAccountsFromOrganizationToPutEvents\",\n      \"Effect\": \"Allow\",\n      \"Principal\": \"*\",\n      \"Action\": \"events:PutEvents\",\n      \"Resource\":\n      \"arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus\",\n      \"Condition\": {\n        \"StringEquals\": {\n          \"aws:PrincipalOrgID\": \"o-ki7yjt看5\"\n        }\n      },\n      \"Sid\":\n      \"AllowAccountToManageRulesTheyCreated\",\n      \"Effect\": \"Allow\",\n      \"Principal\": {\n        \"AWS\":\n        \"arn:aws:iam::123456789012:root\"\n      },\n      \"Action\": [\n        \"events:PutRule\",\n        \"events:PutTargets\",\n        \"events>DeleteRule\",\n        \"events:RemoveTargets\",\n        \"events:DisableRule\",\n        \"events:EnableRule\",\n        \"events:TagResource\",\n        \"events:UntagResource\",\n        \"events:DescribeRule\",\n        \"events>ListTargetsByRule\",\n        \"events>ListTagsForResource\"\n      ],\n      \"Resource\": \"arn:aws:events:us-east-1:123456789012:rule/my-event-bus\",\n      \"Condition\": {\n        \"StringEqualsIfExists\": {\n          \"events:creatorAccount\": \"123456789012\"\n        }\n      }\n    }\n  ]\n}"
```

AwsGuardDutyRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsGuardDuty` Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsGuardDutyDetector

Das `AwsGuardDutyDetector` Objekt liefert Informationen über einen GuardDuty Amazon-Detektor. Ein Detektor ist ein Objekt, das den GuardDuty Service repräsentiert. Ein Detektor ist erforderlich GuardDuty , um betriebsbereit zu sein.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsGuardDutyDetector` Objekt. Beschreibungen der `AwsGuardDutyDetector` Attribute finden Sie [AWSGuardDutyDetector](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsGuardDutyDetector": {
  "FindingPublishingFrequency": "SIX_HOURS",
  "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
  "Status": "ENABLED",
  "DataSources": {
    "CloudTrail": {
      "Status": "ENABLED"
    },
    "DnsLogs": {
      "Status": "ENABLED"
    },
    "FlowLogs": {
      "Status": "ENABLED"
    },
    "S3Logs": {
      "Status": "ENABLED"
    },
    "Kubernetes": {
      "AuditLogs": {
        "Status": "ENABLED"
      }
    },
    "MalwareProtection": {
      "ScanEc2InstanceWithFindings": {
        "EbsVolumes": {
          "Status": "ENABLED"
        }
      },
      "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/malware-
protection.guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDutyMalwareProtection"
    }
  }
}
```

AwsIamRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für AwsIam Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsIamAccessKey

Das AwsIamAccessKey Objekt enthält Details zu einem IAM-Zugriffsschlüssel, der sich auf einen Befund bezieht.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das AwsIamAccessKey Objekt. Beschreibungen der AwsIamAccessKey Attribute finden Sie [AwsIamAccessKeyDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsIamAccessKey": {
    "AccessKeyId": "string",
    "AccountId": "string",
    "CreatedAt": "string",
    "PrincipalId": "string",
    "PrincipalName": "string",
    "PrincipalType": "string",
    "SessionContext": {
        "Attributes": {
            "CreationDate": "string",
            "MfaAuthenticated": boolean
        },
        "SessionIssuer": {
            "AccountId": "string",
            "Arn": "string",
            "PrincipalId": "string",
            "Type": "string",
            "UserName": "string"
        }
    },
    "Status": "string"
}
```

AwsIamGroup

Das `AwsIamGroup` Objekt enthält Details zu einer IAM-Gruppe.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsIamGroup` Objekt. Beschreibungen der `AwsIamGroup` Attribute finden Sie [AwsIamGroupDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsIamGroup": {
  "AttachedManagedPolicies": [
    {
      "PolicyArn": "arn:aws:iam::aws:policy/ExampleManagedAccess",
      "PolicyName": "ExampleManagedAccess",
    }
  ],
  "CreateDate": "2020-04-28T14:08:37.000Z",
  "GroupId": "AGPA4TPS3VLP7QEXAMPLE",
  "GroupName": "Example_User_Group",
  "GroupPolicyList": [
    {
      "PolicyName": "ExampleGroupPolicy"
    }
  ],
  "Path": "/"
}
```

AwsIamPolicy

Das `AwsIamPolicy` Objekt stellt eine IAM-Berechtigungsrichtlinie dar.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsIamPolicy` Objekt. Beschreibungen der `AwsIamPolicy` Attribute finden Sie [AwsIamPolicyDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsIamPolicy": {
  "AttachmentCount": 1,
  "CreateDate": "2017-09-14T08:17:29.000Z",
  "DefaultVersionId": "v1",
}
```

```

    "Description": "Example IAM policy",
    "IsAttachable": true,
    "Path": "/",
    "PermissionsBoundaryUsageCount": 5,
    "PolicyId": "ANPAJ2UCCR6DPCEXAMPLE",
    "PolicyName": "EXAMPLE-MANAGED-POLICY",
    "PolicyVersionList": [
      {
        "VersionId": "v1",
        "IsDefaultVersion": true,
        "CreateDate": "2017-09-14T08:17:29.000Z"
      }
    ],
    "UpdateDate": "2017-09-14T08:17:29.000Z"
  }

```

AwsIamRole

Das `AwsIamRole` Objekt enthält Informationen zu einer IAM-Rolle, einschließlich aller Richtlinien der Rolle.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsIamRole` Objekt. Beschreibungen der `AwsIamRole` Attribute finden Sie [AwsIamRoleDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsIamRole": {
  "AssumeRolePolicyDocument": "{\"Version\": \"2012-10-17\", \"Statement\": [{\"Effect\": \"Allow\", \"Action\": \"sts:AssumeRole\"}]}\",
  "AttachedManagedPolicies": [
    {
      "PolicyArn": "arn:aws:iam::aws:policy/ExamplePolicy1",
      "PolicyName": "Example policy 1"
    },
    {
      "PolicyArn": "arn:aws:iam::444455556666:policy/ExamplePolicy2",
      "PolicyName": "Example policy 2"
    }
  ],
  "CreateDate": "2020-03-14T07:19:14.000Z",
  "InstanceProfileList": [
    {

```

```

    "Arn": "arn:aws:iam::333333333333:ExampleProfile",
    "CreateDate": "2020-03-11T00:02:27Z",
    "InstanceProfileId": "AIPAIXEU4NUHUPEXAMPLE",
    "InstanceProfileName": "ExampleInstanceProfile",
    "Path": "/",
    "Roles": [
      {
        "Arn": "arn:aws:iam::444455556666:role/example-role",
        "AssumeRolePolicyDocument": "",
        "CreateDate": "2020-03-11T00:02:27Z",
        "Path": "/",
        "RoleId": "AR0AJ520TH4H7LEXAMPLE",
        "RoleName": "example-role",
      }
    ]
  },
  "MaxSessionDuration": 3600,
  "Path": "/",
  "PermissionsBoundary": {
    "PermissionsBoundaryArn": "arn:aws:iam::aws:policy/AdministratorAccess",
    "PermissionsBoundaryType": "PermissionsBoundaryPolicy"
  },
  "RoleId": "AR0A4TPS3VLEXAMPLE",
  "RoleName": "BONESBootstrapHydra-OverbridgeOpsFunctionsLambda",
  "RolePolicyList": [
    {
      "PolicyName": "Example role policy"
    }
  ]
}

```

AwsIamUser

Das `AwsIamUser` Objekt stellt Informationen über einen Benutzer bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsIamUser` Objekt. Beschreibungen der `AwsIamUser` Attribute finden Sie [AwsIamUserDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsIamUser": {
```



```

    "AttachedManagedPolicies": [
      {
        "PolicyName": "ExamplePolicy",
        "PolicyArn": "arn:aws:iam::aws:policy/ExampleAccess"
      }
    ],
    "CreateDate": "2018-01-26T23:50:05.000Z",
    "GroupList": [],
    "Path": "/",
    "PermissionsBoundary" : {
      "PermissionsBoundaryArn" : "arn:aws:iam::aws:policy/AdministratorAccess",
      "PermissionsBoundaryType" : "PermissionsBoundaryPolicy"
    },
    "UserId": "AIDACKCEVSQ6C2EXAMPLE",
    "UserName": "ExampleUser",
    "UserPolicyList": [
      {
        "PolicyName": "InstancePolicy"
      }
    ]
  }
}

```

AwsKinesisRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsKinesis` Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsKinesisStream

Das `AwsKinesisStream` Objekt enthält Details zu Amazon Kinesis Data Streams.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsKinesisStream` Objekt. Beschreibungen der `AwsKinesisStream` Attribute finden Sie [AwsKinesisStreamDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsKinesisStream": {
  "Name": "test-vir-kinesis-stream",
  "Arn": "arn:aws:kinesis:us-east-1:293279581038:stream/test-vir-kinesis-stream",

```

```
"RetentionPeriodHours": 24,  
"ShardCount": 2,  
"StreamEncryption": {  
  "EncryptionType": "KMS",  
  "KeyId": "arn:aws:kms:us-east-1:293279581038:key/849cf029-4143-4c59-91f8-  
ea76007247eb"  
}  
}
```

AwsKmsRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für AwsKms Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter. [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsKmsKey

Das AwsKmsKey Objekt enthält Details zu einem AWS KMS key.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das AwsKmsKey Objekt. Beschreibungen der AwsKmsKey Attribute finden Sie [AwsKmsKeyDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsKmsKey": {  
  "AWSAccountId": "string",  
  "CreationDate": "string",  
  "Description": "string",  
  "KeyId": "string",  
  "KeyManager": "string",  
  "KeyRotationStatus": boolean,  
  "KeyState": "string",  
  "Origin": "string"  
}
```

AwsLambda

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für AwsLambda Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter: [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsLambdaFunction

Das `AwsLambdaFunction` Objekt enthält Details zur Konfiguration einer Lambda-Funktion.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsLambdaFunction` Objekt. Beschreibungen der `AwsLambdaFunction` Attribute finden Sie [AwsLambdaFunctionDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsLambdaFunction": {
  "Architectures": [
    "x86_64"
  ],
  "Code": {
    "S3Bucket": "amzn-s3-demo-bucket",
    "S3Key": "samplekey",
    "S3ObjectVersion": "2",
    "ZipFile": "myzip.zip"
  },
  "CodeSha256": "1111111111111111abcdef",
  "DeadLetterConfig": {
    "TargetArn": "arn:aws:lambda:us-east-2:123456789012:queue:myqueue:2"
  },
  "Environment": {
    "Variables": {
      "Stage": "foobar"
    },
    "Error": {
      "ErrorCode": "Sample-error-code",
      "Message": "Caller principal is a manager."
    }
  },
  "FunctionName": "CheckOut",
  "Handler": "main.py:lambda_handler",
  "KmsKeyArn": "arn:aws:kms:us-west-2:123456789012:key/mykey",
  "LastModified": "2001-09-11T09:00:00Z",
  "Layers": {
    "Arn": "arn:aws:lambda:us-east-2:123456789012:layer:my-layer:3",
    "CodeSize": 169
  }
}
```

```

    },
    "PackageType": "Zip",
    "RevisionId": "23",
    "Role": "arn:aws:iam::123456789012:role/Accounting-Role",
    "Runtime": "go1.7",
    "Timeout": 15,
    "TracingConfig": {
        "Mode": "Active"
    },
    },
    "Version": "$LATEST$",
    "VpcConfig": {
        "SecurityGroupIds": ["sg-085912345678492fb", "sg-08591234567bdgdc"],
        "SubnetIds": ["subnet-071f712345678e7c8", "subnet-07fd123456788a036"]
    },
    },
    "MasterArn": "arn:aws:lambda:us-east-2:123456789012:\$LATEST",
    "MemorySize": 2048
}

```

AwsLambdaLayerVersion

Das `AwsLambdaLayerVersion` Objekt enthält Details zu einer Lambda-Layer-Version.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsLambdaLayerVersion` Objekt. Beschreibungen der `AwsLambdaLayerVersion` Attribute finden Sie [AWSLambdaLayerVersionDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsLambdaLayerVersion": {
    "Version": 2,
    "CompatibleRuntimes": [
        "java8"
    ],
    "CreateDate": "2019-10-09T22:02:00.274+0000"
}

```

AwsMskRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsMsk` Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsMskCluster

Das `AwsMskCluster` Objekt stellt Informationen über einen Amazon Managed Streaming for Apache Kafka (Amazon MSK) -Cluster bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt.

`AwsMskCluster` Beschreibungen der `AwsMskCluster` Attribute finden Sie [AwsMskClusterDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsMskCluster": {
  "ClusterInfo": {
    "ClientAuthentication": {
      "Sasl": {
        "Scram": {
          "Enabled": true
        },
        "Iam": {
          "Enabled": true
        }
      },
      "Tls": {
        "CertificateAuthorityArnList": [],
        "Enabled": false
      },
      "Unauthenticated": {
        "Enabled": false
      }
    },
    "ClusterName": "my-cluster",
    "CurrentVersion": "K2PWKAKR8XB7XF",
    "EncryptionInfo": {
      "EncryptionAtRest": {
        "DataVolumeKMSKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
      },
      "EncryptionInTransit": {
        "ClientBroker": "TLS",
        "InCluster": true
      }
    },
    "EnhancedMonitoring": "PER_TOPIC_PER_BROKER",
```

```

      "NumberOfBrokerNodes": 3
    }
  }
}

```

AwsNetworkFirewallRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsNetworkFirewall` Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter. [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsNetworkFirewallFirewall

Das `AwsNetworkFirewallFirewall` Objekt enthält Details zu einer AWS Network Firewall Firewall.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsNetworkFirewallFirewall` Objekt. Beschreibungen der `AwsNetworkFirewallFirewall` Attribute finden Sie [AwsNetworkFirewallFirewallDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsNetworkFirewallFirewall": {
  "DeleteProtection": false,
  "FirewallArn": "arn:aws:network-firewall:us-east-1:024665936331:firewall/testfirewall",
  "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-policy/InitialFirewall",
  "FirewallId": "dea7d8e9-ae38-4a8a-b022-672a830a99fa",
  "FirewallName": "testfirewall",
  "FirewallPolicyChangeProtection": false,
  "SubnetChangeProtection": false,
  "SubnetMappings": [
    {
      "SubnetId": "subnet-0183481095e588cdc"
    },
    {
      "SubnetId": "subnet-01f518fad1b1c90b0"
    }
  ],
  "VpcId": "vpc-40e83c38"
}

```

```
}
```

AwsNetworkFirewallFirewallPolicy

Das `AwsNetworkFirewallFirewallPolicy` Objekt enthält Details zu einer Firewall-Richtlinie. Eine Firewall-Richtlinie definiert das Verhalten einer Netzwerk-Firewall.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsNetworkFirewallFirewallPolicy` Objekt. Beschreibungen der `AwsNetworkFirewallFirewallPolicy` Attribute finden Sie [AWSNetworkFirewallFirewallPolicyDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsNetworkFirewallFirewallPolicy": {
  "FirewallPolicy": {
    "StatefulRuleGroupReferences": [
      {
        "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-
rulegroup/PatchesOnly"
      }
    ],
    "StatelessDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessFragmentDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessRuleGroupReferences": [
      {
        "Priority": 1,
        "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-
rulegroup/Stateless-1"
      }
    ]
  },
  "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-
policy/InitialFirewall",
  "FirewallPolicyId": "9ceeda22-6050-4048-a0ca-50ce47f0cc65",
  "FirewallPolicyName": "InitialFirewall",
  "Description": "Initial firewall"
}
```

AwsNetworkFirewallRuleGroup

Das `AwsNetworkFirewallRuleGroup` Objekt enthält Details zu einer AWS Network Firewall Regelgruppe. Regelgruppen werden verwendet, um den Netzwerkverkehr zu untersuchen und zu

kontrollieren. Zustandslose Regelgruppen gelten für einzelne Pakete. Stateful-Regelgruppen gelten für Pakete im Kontext ihres Datenverkehrs.

Auf Regelgruppen wird in Firewallrichtlinien verwiesen.

Die folgenden Beispiele zeigen das AWS Security Finding Format (ASFF) für das `AwsNetworkFirewallRuleGroup` Objekt. Beschreibungen der `AwsNetworkFirewallRuleGroup` Attribute finden Sie [AWSNetworkFirewallRuleGroupDetails](#) in der AWS Security Hub API-Referenz.

Beispiel — Regelgruppe ohne Status

```
"AwsNetworkFirewallRuleGroup": {
  "Capacity": 600,
  "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-rulegroup/Stateless-1",
  "RuleGroupId": "fb13c4df-b6da-4c1e-91ec-84b7a5487493",
  "RuleGroupName": "Stateless-1"
  "Description": "Example of a stateless rule group",
  "Type": "STATELESS",
  "RuleGroup": {
    "RulesSource": {
      "StatelessRulesAndCustomActions": {
        "CustomActions": [],
        "StatelessRules": [
          {
            "Priority": 1,
            "RuleDefinition": {
              "Actions": [
                "aws:pass"
              ],
              "MatchAttributes": {
                "DestinationPorts": [
                  {
                    "FromPort": 443,
                    "ToPort": 443
                  }
                ],
                "Destinations": [
                  {
                    "AddressDefinition": "192.0.2.0/24"
                  }
                ]
              }
            }
          }
        ]
      }
    }
  }
}
```



```
        "Protocols": [
            6
        ],
        "SourcePorts": [
            {
                "FromPort": 0,
                "ToPort": 65535
            }
        ],
        "Sources": [
            {
                "AddressDefinition": "198.51.100.0/24"
            }
        ]
    }
}
}
```

Beispiel — Regelgruppe mit Status

```
"AwsNetworkFirewallRuleGroup": {
  "Capacity": 100,
  "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-
rulegroup/tupletest",
  "RuleGroupId": "38b71c12-da80-4643-a6c5-03337f8933e0",
  "RuleGroupName": "ExampleRuleGroup",
  "Description": "Example of a stateful rule group",
  "Type": "STATEFUL",
  "RuleGroup": {
    "RuleSource": {
      "StatefulRules": [
        {
          "Action": "PASS",
          "Header": {
            "Destination": "Any",
            "DestinationPort": "443",
            "Direction": "ANY",
            "Protocol": "TCP",
```

```

        "Source": "Any",
        "SourcePort": "Any"
      },
      "RuleOptions": [
        {
          "Keyword": "sid:1"
        }
      ]
    }
  ]
}

```

Im Folgenden finden Sie eine Liste mit Beispielen für gültige Werte für `AwsNetworkFirewallRuleGroup` Attribute:

- Action

Zulässige Werte: PASS | DROP | ALERT

- Protocol

Gültige Werte: IP TCP | UDP | ICMP | HTTP | FTP | TLS | SMB | DNS | DCERPC | SSH | SMTP | IMAP | MSN | KRB5 | IKEV2 | TFTP | NTP | DHCP

- Flags

Zulässige Werte: FIN | SYN | RST | PSH | ACK | URG | ECE | CWR

- Masks

Zulässige Werte: FIN | SYN | RST | PSH | ACK | URG | ECE | CWR

AwsOpenSearchServiceRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsOpenSearchService` Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter. [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsOpenSearchServiceDomain

Das `AwsOpenSearchServiceDomain` Objekt enthält Informationen über eine Amazon OpenSearch Service-Domain.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsOpenSearchServiceDomain` Objekt. Beschreibungen der `AwsOpenSearchServiceDomain` Attribute finden Sie [AWSOpenSearchServiceDomainDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsOpenSearchServiceDomain": {
  "AccessPolicies": "IAM_Id",
  "AdvancedSecurityOptions": {
    "Enabled": true,
    "InternalUserDatabaseEnabled": true,
    "MasterUserOptions": {
      "MasterUserArn": "arn:aws:iam::123456789012:user/third-master-use",
      "MasterUserName": "third-master-use",
      "MasterUserPassword": "some-password"
    }
  },
  "Arn": "arn:aws:opensearch:us-east-1:111122223333:somedomain",
  "ClusterConfig": {
    "InstanceType": "c5.large.search",
    "InstanceCount": 1,
    "DedicatedMasterEnabled": true,
    "ZoneAwarenessEnabled": false,
    "ZoneAwarenessConfig": {
      "AvailabilityZoneCount": 2
    },
    "DedicatedMasterType": "c5.large.search",
    "DedicatedMasterCount": 3,
    "WarmEnabled": true,
    "WarmCount": 3,
    "WarmType": "ultrawarm1.large.search"
  },
  "DomainEndpoint": "https://es-2021-06-23t17-04-qowmgghud5vofgb5e4wmi.eu-central-1.es.amazonaws.com",
  "DomainEndpointOptions": {
    "EnforceHTTPS": false,
    "TLSecurityPolicy": "Policy-Min-TLS-1-0-2019-07",
```

```

    "CustomEndpointCertificateArn": "arn:aws:acm:us-east-1:111122223333:certificate/bda1bff1-79c0-49d0-abe6-50a15a7477d4",
    "CustomEndpointEnabled": true,
    "CustomEndpoint": "example.com"
  },
  "DomainEndpoints": {
    "vpc": "vpc-endpoint-h2dsd34efgyghrtguk5gt6j2foh4.us-east-1.es.amazonaws.com"
  },
  "DomainName": "my-domain",
  "EncryptionAtRestOptions": {
    "Enabled": false,
    "KmsKeyId": "1a2a3a4-1a2a-3a4a-5a6a-1a2a3a4a5a6a"
  },
  "EngineVersion": "7.1",
  "Id": "123456789012",
  "LogPublishingOptions": {
    "IndexSlowLogs": {
      "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-group:/aws/aes/domains/es-index-slow-logs",
      "Enabled": true
    },
    "SearchSlowLogs": {
      "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-group:/aws/aes/domains/es-slow-logs",
      "Enabled": true
    },
    "AuditLogs": {
      "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-group:/aws/aes/domains/es-slow-logs",
      "Enabled": true
    }
  },
  "NodeToNodeEncryptionOptions": {
    "Enabled": true
  },
  "ServiceSoftwareOptions": {
    "AutomatedUpdateDate": "2022-04-28T14:08:37.000Z",
    "Cancellable": false,
    "CurrentVersion": "R20210331",
    "Description": "There is no software update available for this domain.",
    "NewVersion": "OpenSearch_1.0",
    "UpdateAvailable": false,
    "UpdateStatus": "COMPLETED",
    "OptionalDeployment": false
  }
}

```

```

    },
    "VpcOptions": {
      "SecurityGroupIds": [
        "sg-2a3a4a5a"
      ],
      "SubnetIds": [
        "subnet-1a2a3a4a"
      ],
    }
  }
}

```

AwsRdsRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für AwsRds Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsRdsDbCluster

Das `AwsRdsDbCluster` Objekt enthält Details zu einem Amazon RDS-Datenbankcluster.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsRdsDbCluster` Objekt. Beschreibungen der `AwsRdsDbCluster` Attribute finden Sie [AwsRdsDbClusterDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsRdsDbCluster": {
  "ActivityStreamStatus": "stopped",
  "AllocatedStorage": 1,
  "AssociatedRoles": [
    {
      "RoleArn": "arn:aws:iam::777788889999:role/aws-service-role/rds.amazonaws.com/AWSServiceRoleForRDS",
      "Status": "PENDING"
    }
  ],
  "AutoMinorVersionUpgrade": true,
  "AvailabilityZones": [
    "us-east-1a",
    "us-east-1c",

```

```

    "us-east-1e"
  ],
  "BackupRetentionPeriod": 1,
  "ClusterCreateTime": "2020-06-22T17:40:12.322Z",
  "CopyTagsToSnapshot": true,
  "CrossAccountClone": false,
  "CustomEndpoints": [],
  "DatabaseName": "Sample name",
  "DbClusterIdentifier": "database-3",
  "DbClusterMembers": [
    {
      "DbClusterParameterGroupStatus": "in-sync",
      "DbInstanceIdentifier": "database-3-instance-1",
      "IsClusterWriter": true,
      "PromotionTier": 1,
    }
  ],
  "DbClusterOptionGroupMemberships": [],
  "DbClusterParameterGroup": "cluster-parameter-group",
  "DbClusterResourceId": "cluster-example",
  "DbSubnetGroup": "subnet-group",
  "DeletionProtection": false,
  "DomainMemberships": [],
  "Status": "modifying",
  "EnabledCloudwatchLogsExports": [
    "audit",
    "error",
    "general",
    "slowquery"
  ],
  "Endpoint": "database-3.cluster-example.us-east-1.rds.amazonaws.com",
  "Engine": "aurora-mysql",
  "EngineMode": "provisioned",
  "EngineVersion": "5.7.mysql_aurora.2.03.4",
  "HostedZoneId": "ZONE1",
  "HttpEndpointEnabled": false,
  "IamDatabaseAuthenticationEnabled": false,
  "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
  "MasterUsername": "admin",
  "MultiAz": false,
  "Port": 3306,
  "PreferredBackupWindow": "04:52-05:22",
  "PreferredMaintenanceWindow": "sun:09:32-sun:10:02",
  "ReaderEndpoint": "database-3.cluster-ro-example.us-east-1.rds.amazonaws.com",

```

```

    "ReadReplicaIdentifiers": [],
    "Status": "Modifying",
    "StorageEncrypted": true,
    "VpcSecurityGroups": [
      {
        "Status": "active",
        "VpcSecurityGroupId": "sg-example-1"
      }
    ],
  },
}

```

AwsRdsDbClusterSnapshot

Das `AwsRdsDbClusterSnapshot` Objekt enthält Informationen über einen Amazon RDS-DB-Cluster-Snapshot.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsRdsDbClusterSnapshot` Objekt. Beschreibungen der `AwsRdsDbClusterSnapshot` Attribute finden Sie [AwsRdsDbClusterSnapshotDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsRdsDbClusterSnapshot": {
  "AllocatedStorage": 0,
  "AvailabilityZones": [
    "us-east-1a",
    "us-east-1d",
    "us-east-1e"
  ],
  "ClusterCreateTime": "2020-06-12T13:23:15.577Z",
  "DbClusterIdentifier": "database-2",
  "DbClusterSnapshotAttributes": [{
    "AttributeName": "restore",
    "AttributeValues": ["123456789012"]
  }],
  "DbClusterSnapshotIdentifier": "rds:database-2-2020-06-23-03-52",
  "Engine": "aurora",
  "EngineVersion": "5.6.10a",
  "IamDatabaseAuthenticationEnabled": false,
  "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
  "LicenseModel": "aurora",
  "MasterUsername": "admin",
  "PercentProgress": 100,
}

```

```

    "Port": 0,
    "SnapshotCreateTime": "2020-06-22T17:40:12.322Z",
    "SnapshotType": "automated",
    "Status": "available",
    "StorageEncrypted": true,
    "VpcId": "vpc-faf7e380"
  }

```

AwsRdsDbInstance

Das `AwsRdsDbInstance` Objekt enthält Details zu einer Amazon RDS-DB-Instance.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsRdsDbInstance` Objekt. Beschreibungen der `AwsRdsDbInstance` Attribute finden Sie [AwsRdsDbInstanceDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsRdsDbInstance": {
  "AllocatedStorage": 20,
  "AssociatedRoles": [],
  "AutoMinorVersionUpgrade": true,
  "AvailabilityZone": "us-east-1d",
  "BackupRetentionPeriod": 7,
  "CaCertificateIdentifier": "certificate1",
  "CharacterSetName": "",
  "CopyTagsToSnapshot": true,
  "DbClusterIdentifier": "",
  "DbInstanceArn": "arn:aws:rds:us-east-1:111122223333:db:database-1",
  "DbInstanceClass": "db.t2.micro",
  "DbInstanceIdentifier": "database-1",
  "DbInstancePort": 0,
  "DbInstanceStatus": "available",
  "DbiResourceId": "db-EXAMPLE123",
  "DbName": "",
  "DbParameterGroups": [
    {
      "DbParameterGroupName": "default.mysql5.7",
      "ParameterApplyStatus": "in-sync"
    }
  ],

```



```

"DbSecurityGroups": [],

"DbSubnetGroup": {
  "DbSubnetGroupName": "my-group-123abc",
  "DbSubnetGroupDescription": "My subnet group",
  "VpcId": "vpc-example1",
  "SubnetGroupStatus": "Complete",
  "Subnets": [
    {
      "SubnetIdentifier": "subnet-123abc",
      "SubnetAvailabilityZone": {
        "Name": "us-east-1d"
      },
      "SubnetStatus": "Active"
    },
    {
      "SubnetIdentifier": "subnet-456def",
      "SubnetAvailabilityZone": {
        "Name": "us-east-1c"
      },
      "SubnetStatus": "Active"
    }
  ],
  "DbSubnetGroupArn": ""
},
"DeletionProtection": false,
"DomainMemberships": [],
"EnabledCloudWatchLogsExports": [],
"Endpoint": {
  "address": "database-1.example.us-east-1.rds.amazonaws.com",
  "port": 3306,
  "hostedZoneId": "ZONEID1"
},
"Engine": "mysql",
"EngineVersion": "5.7.22",
"EnhancedMonitoringResourceArn": "arn:aws:logs:us-east-1:111122223333:log-group:Example:log-stream:db-EXAMPLE1",
"IamDatabaseAuthenticationEnabled": false,
"InstanceCreateTime": "2020-06-22T17:40:12.322Z",
"Iops": "",
"KmsKeyId": "",
"LatestRestorableTime": "2020-06-24T05:50:00.000Z",
"LicenseModel": "general-public-license",

```

```

"ListenerEndpoint": "",
"MasterUsername": "admin",
"MaxAllocatedStorage": 1000,
"MonitoringInterval": 60,
"MonitoringRoleArn": "arn:aws:iam::111122223333:role/rds-monitoring-role",
"MultiAz": false,
"OptionGroupMemberships": [
  {
    "OptionGroupName": "default:mysql-5-7",
    "Status": "in-sync"
  }
],
"PreferredBackupWindow": "03:57-04:27",
"PreferredMaintenanceWindow": "thu:10:13-thu:10:43",
"PendingModifiedValues": {
  "DbInstanceClass": "",
  "AllocatedStorage": "",
  "MasterUserPassword": "",
  "Port": "",
  "BackupRetentionPeriod": "",
  "MultiAZ": "",
  "EngineVersion": "",
  "LicenseModel": "",
  "Iops": "",
  "DbInstanceIdentifier": "",
  "StorageType": "",
  "CaCertificateIdentifier": "",
  "DbSubnetGroupName": "",
  "PendingCloudWatchLogsExports": "",
  "ProcessorFeatures": []
},
"PerformanceInsightsEnabled": false,
"PerformanceInsightsKmsKeyId": "",
"PerformanceInsightsRetentionPeriod": "",
"ProcessorFeatures": [],
"PromotionTier": "",
"PubliclyAccessible": false,
"ReadReplicaDBClusterIdentifiers": [],
"ReadReplicaDBInstanceIdentifiers": [],
"ReadReplicaSourceDBInstanceIdentifier": "",
"SecondaryAvailabilityZone": "",
"StatusInfos": [],
"StorageEncrypted": false,
"StorageType": "gp2",

```

```

    "TdeCredentialArn": "",
    "Timezone": "",
    "VpcSecurityGroups": [
      {
        "VpcSecurityGroupId": "sg-example1",
        "Status": "active"
      }
    ]
  }
}

```

AwsRdsDbSecurityGroup

Das `AwsRdsDbSecurityGroup` Objekt enthält Informationen über einen Amazon Relational Database Service

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsRdsDbSecurityGroup` Objekt. Beschreibungen der `AwsRdsDbSecurityGroup` Attribute finden Sie [AwsRdsDbSecurityGroupDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsRdsDbSecurityGroup": {
  "DbSecurityGroupArn": "arn:aws:rds:us-west-1:111122223333:secgrp:default",
  "DbSecurityGroupDescription": "default",
  "DbSecurityGroupName": "mysecgroup",
  "Ec2SecurityGroups": [
    {
      "Ec2SecurityGroupuId": "myec2group",
      "Ec2SecurityGroupName": "default",
      "Ec2SecurityGroupOwnerId": "987654321021",
      "Status": "authorizing"
    }
  ],
  "IpRanges": [
    {
      "Cidrip": "0.0.0.0/0",
      "Status": "authorizing"
    }
  ],
  "OwnerId": "123456789012",
  "VpcId": "vpc-1234567f"
}

```

AwsRdsDbSnapshot

Das `AwsRdsDbSnapshot` Objekt enthält Details zu einem Amazon RDS-DB-Cluster-Snapshot.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsRdsDbSnapshot` Objekt. Beschreibungen der `AwsRdsDbSnapshot` Attribute finden Sie [AwsRdsDbSnapshotDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsRdsDbSnapshot": {
  "DbSnapshotIdentifier": "rds:database-1-2020-06-22-17-41",
  "DbInstanceIdentifier": "database-1",
  "SnapshotCreateTime": "2020-06-22T17:41:29.967Z",
  "Engine": "mysql",
  "AllocatedStorage": 20,
  "Status": "available",
  "Port": 3306,
  "AvailabilityZone": "us-east-1d",
  "VpcId": "vpc-example1",
  "InstanceCreateTime": "2020-06-22T17:40:12.322Z",
  "MasterUsername": "admin",
  "EngineVersion": "5.7.22",
  "LicenseModel": "general-public-license",
  "SnapshotType": "automated",
  "Iops": null,
  "OptionGroupName": "default:mysql-5-7",
  "PercentProgress": 100,
  "SourceRegion": null,
  "SourceDbSnapshotIdentifier": "",
  "StorageType": "gp2",
  "TdeCredentialArn": "",
  "Encrypted": false,
  "KmsKeyId": "",
  "Timezone": "",
  "IamDatabaseAuthenticationEnabled": false,
  "ProcessorFeatures": [],
  "DbiResourceId": "db-resourceexample1"
}
```

AwsRdsEventSubscription

Das `AwsRdsEventSubscription` enthält Einzelheiten zu einem Abonnement für RDS-Ereignisbenachrichtigungen. Das Abonnement ermöglicht es RDS, Ereignisse zu einem SNS-Thema zu veröffentlichen.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsRdsEventSubscription` Objekt. Beschreibungen der `AwsRdsEventSubscription` Attribute finden Sie [AwsRdsEventSubscriptionDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsRdsEventSubscription": {
  "CustSubscriptionId": "myawsuser-secgrp",
  "CustomerAwsId": "111111111111",
  "Enabled": true,
  "EventCategoriesList": [
    "configuration change",
    "failure"
  ],
  "EventSubscriptionArn": "arn:aws:rds:us-east-1:111111111111:es:my-instance-events",
  "SnsTopicArn": "arn:aws:sns:us-east-1:111111111111:myawsuser-RDS",
  "SourceIdsList": [
    "si-sample",
    "mysqlldb-rr"
  ],
  "SourceType": "db-security-group",
  "Status": "creating",
  "SubscriptionCreationTime": "2021-06-27T01:38:01.090Z"
}
```

AwsRedshiftRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsRedshift` Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsRedshiftCluster

Das `AwsRedshiftCluster` Objekt enthält Details zu einem Amazon Redshift Redshift-Cluster.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsRedshiftCluster` Objekt. Beschreibungen der `AwsRedshiftCluster` Attribute finden Sie [AWSRedshiftClusterDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsRedshiftCluster": {
  "AllowVersionUpgrade": true,
  "AutomatedSnapshotRetentionPeriod": 1,
  "AvailabilityZone": "us-west-2d",
  "ClusterAvailabilityStatus": "Unavailable",
  "ClusterCreateTime": "2020-08-03T19:22:44.637Z",
  "ClusterIdentifier": "redshift-cluster-1",
  "ClusterNodes": [
    {
      "NodeRole": "LEADER",
      "PrivateIPAddress": "192.0.2.108",
      "PublicIPAddress": "198.51.100.29"
    },
    {
      "NodeRole": "COMPUTE-0",
      "PrivateIPAddress": "192.0.2.22",
      "PublicIPAddress": "198.51.100.63"
    },
    {
      "NodeRole": "COMPUTE-1",
      "PrivateIPAddress": "192.0.2.224",
      "PublicIPAddress": "198.51.100.226"
    }
  ],
  "ClusterParameterGroups": [
    {
      "ClusterParameterStatusList": [
        {
          "ParameterName": "max_concurrency_scaling_clusters",
          "ParameterApplyStatus": "in-sync",
          "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
        },
        {
          "ParameterName": "enable_user_activity_logging",
          "ParameterApplyStatus": "in-sync",
          "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
        }
      ]
    }
  ]
}
```

```
{
  "ParameterName": "auto_analyze",
  "ParameterApplyStatus": "in-sync",
  "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
},
{
  "ParameterName": "query_group",
  "ParameterApplyStatus": "in-sync",
  "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
},
{
  "ParameterName": "datestyle",
  "ParameterApplyStatus": "in-sync",
  "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
},
{
  "ParameterName": "extra_float_digits",
  "ParameterApplyStatus": "in-sync",
  "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
},
{
  "ParameterName": "search_path",
  "ParameterApplyStatus": "in-sync",
  "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
},
{
  "ParameterName": "statement_timeout",
  "ParameterApplyStatus": "in-sync",
  "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
},
{
  "ParameterName": "wlm_json_configuration",
  "ParameterApplyStatus": "in-sync",
  "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
},
{
  "ParameterName": "require_ssl",
  "ParameterApplyStatus": "in-sync",
  "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
},
{
  "ParameterName": "use_fips_ssl",
  "ParameterApplyStatus": "in-sync",
  "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
}
```

```

        }
    ],
    "ParameterApplyStatus": "in-sync",
    "ParameterGroupName": "temp"
}
],
"ClusterPublicKey": "Ja1rXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY Amazon-Redshift",
"ClusterRevisionNumber": 17498,
"ClusterSecurityGroups": [
    {
        "ClusterSecurityGroupName": "default",
        "Status": "active"
    }
],
"ClusterSnapshotCopyStatus": {
    "DestinationRegion": "us-west-2",
    "ManualSnapshotRetentionPeriod": -1,
    "RetentionPeriod": 1,
    "SnapshotCopyGrantName": "snapshotCopyGrantName"
},
"ClusterStatus": "available",
"ClusterSubnetGroupName": "default",
"ClusterVersion": "1.0",
"DBName": "dev",
"DeferredMaintenanceWindows": [
    {
        "DeferMaintenanceEndTime": "2020-10-07T20:34:01.000Z",
        "DeferMaintenanceIdentifier": "deferMaintenanceIdentifier",
        "DeferMaintenanceStartTime": "2020-09-07T20:34:01.000Z"
    }
],
"ElasticIpStatus": {
    "ElasticIp": "203.0.113.29",
    "Status": "active"
},
"ElasticResizeNumberOfNodeOptions": "4",
"Encrypted": false,
"Endpoint": {
    "Address": "redshift-cluster-1.example.us-west-2.redshift.amazonaws.com",
    "Port": 5439
},
"EnhancedVpcRouting": false,
"ExpectedNextSnapshotScheduleTime": "2020-10-13T20:34:01.000Z",
"ExpectedNextSnapshotScheduleTimeStatus": "OnTrack",

```



```

"HsmStatus": {
  "HsmClientCertificateIdentifier": "hsmClientCertificateIdentifier",
  "HsmConfigurationIdentifier": "hsmConfigurationIdentifier",
  "Status": "applying"
},
"IamRoles": [
  {
    "ApplyStatus": "in-sync",
    "IamRoleArn": "arn:aws:iam::111122223333:role/RedshiftCopyUnload"
  }
],
"KmsKeyId": "kmsKeyId",
"LoggingStatus": {
  "BucketName": "amzn-s3-demo-bucket",
  "LastFailureMessage": "test message",
  "LastFailureTime": "2020-08-09T13:00:00.000Z",
  "LastSuccessfulDeliveryTime": "2020-08-08T13:00:00.000Z",
  "LoggingEnabled": true,
  "S3KeyPrefix": "/"
},
"MaintenanceTrackName": "current",
"ManualSnapshotRetentionPeriod": -1,
"MasterUsername": "awsuser",
"NextMaintenanceWindowStartTime": "2020-08-09T13:00:00.000Z",
"NodeType": "dc2.large",
"NumberOfNodes": 2,
"PendingActions": [],
"PendingModifiedValues": {
  "AutomatedSnapshotRetentionPeriod": 0,
  "ClusterIdentifier": "clusterIdentifier",
  "ClusterType": "clusterType",
  "ClusterVersion": "clusterVersion",
  "EncryptionType": "None",
  "EnhancedVpcRouting": false,
  "MaintenanceTrackName": "maintenanceTrackName",
  "MasterUserPassword": "masterUserPassword",
  "NodeType": "dc2.large",
  "NumberOfNodes": 1,
  "PubliclyAccessible": true
},
"PreferredMaintenanceWindow": "sun:13:00-sun:13:30",
"PubliclyAccessible": true,
"ResizeInfo": {
  "AllowCancelResize": true,

```

```

    "ResizeType": "ClassicResize"
  },
  "RestoreStatus": {
    "CurrentRestoreRateInMegaBytesPerSecond": 15,
    "ElapsedTimeInSeconds": 120,
    "EstimatedTimeToCompletionInSeconds": 100,
    "ProgressInMegaBytes": 10,
    "SnapshotSizeInMegaBytes": 1500,
    "Status": "restoring"
  },
  "SnapshotScheduleIdentifier": "snapshotScheduleIdentifier",
  "SnapshotScheduleState": "ACTIVE",
  "VpcId": "vpc-example",
  "VpcSecurityGroups": [
    {
      "Status": "active",
      "VpcSecurityGroupId": "sg-example"
    }
  ]
}

```

AwsRoute53Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für AwsRoute53 Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsRoute53HostedZone

Das AwsRoute53HostedZone Objekt stellt Informationen über eine von Amazon Route 53 gehostete Zone bereit, einschließlich der vier Nameserver, die der Hosting-Zone zugewiesen sind. Eine gehostete Zone stellt eine Sammlung von Datensätzen dar, die zusammen verwaltet werden können und zu einem einzigen übergeordneten Domainnamen gehören.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das AwsRoute53HostedZone Objekt. Beschreibungen der AwsRoute53HostedZone Attribute finden Sie unter [AwsRoute53 HostedZoneDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsRoute53HostedZone": {

```

```

    "HostedZone": {
      "Id": "Z06419652JEMG09TA2XKL",
      "Name": "asff.testing",
      "Config": {
        "Comment": "This is an example comment."
      }
    },
    "NameServers": [
      "ns-470.awsdns-32.net",
      "ns-1220.awsdns-12.org",
      "ns-205.awsdns-13.com",
      "ns-1960.awsdns-51.co.uk"
    ],
    "QueryLoggingConfig": {
      "CloudWatchLogsLogGroupArn": {
        "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:123456789012:log-
group:asfftesting:*",
        "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "HostedZoneId": "Z00932193AF5H180PPNZD"
      }
    },
    "Vpcs": [
      {
        "Id": "vpc-05d7c6e36bc03ea76",
        "Region": "us-east-1"
      }
    ]
  }

```

AwsS3Ressourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für AwsS3 Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter. [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsS3AccessPoint

AwsS3AccessPointbietet Informationen über einen Amazon S3 S3-Zugriffspunkt. S3-Zugriffspunkte sind benannte Netzwerkendpunkte, die an S3-Buckets angeschlossen sind, mit denen Sie S3-Objektoperationen ausführen können.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt.

AwsS3AccessPoint Beschreibungen der *AwsS3AccessPoint* Attribute finden Sie unter [awSS3AccessPointDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsS3AccessPoint": {
  "AccessPointArn": "arn:aws:s3:us-east-1:123456789012:accesspoint/asff-access-point",
  "Alias": "asff-access-point-hrzrlukc5m36ft7okagglf3gmwluquse1b-s3alias",
  "Bucket": "amzn-s3-demo-bucket",
  "BucketAccountId": "123456789012",
  "Name": "asff-access-point",
  "NetworkOrigin": "VPC",
  "PublicAccessBlockConfiguration": {
    "BlockPublicAcls": true,
    "BlockPublicPolicy": true,
    "IgnorePublicAcls": true,
    "RestrictPublicBuckets": true
  },
  "VpcConfiguration": {
    "VpcId": "vpc-1a2b3c4d5e6f1a2b3"
  }
}
```

AwsS3AccountPublicAccessBlock

AwsS3AccountPublicAccessBlock bietet Informationen zur Amazon S3 Public Access Block-Konfiguration für Konten.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das *AwsS3AccountPublicAccessBlock* Objekt. Beschreibungen der *AwsS3AccountPublicAccessBlock* Attribute finden Sie unter [awSS3AccountPublicAccessBlockDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsS3AccountPublicAccessBlock": {
  "BlockPublicAcls": true,
  "BlockPublicPolicy": true,
  "IgnorePublicAcls": false,
  "RestrictPublicBuckets": true
}
```

}

AwsS3Bucket

Das `AwsS3Bucket` Objekt enthält Details zu einem Amazon S3 S3-Bucket.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsS3Bucket` Objekt. Beschreibungen der `AwsS3Bucket` Attribute finden Sie unter [awSS3 BucketDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsS3Bucket": {
  "AccessControlList": "{ \"grantSet\": null, \"grantList\": [ { \"grantee\": { \"id\": \"4df55416215956920d9d056aa8b99803a294ea221222bb668b55a8c6bca81094\", \"displayName\": null }, \"permission\": \"FullControl\" }, { \"grantee\": \"AllUsers\", \"permission\": \"ReadAcp\" }, { \"grantee\": \"AuthenticatedUsers\", \"permission\": \"ReadAcp\" } ], \"BucketLifecycleConfiguration\": {
    \"Rules\": [
      {
        \"AbortIncompleteMultipartUpload\": {
          \"DaysAfterInitiation\": 5
        },
        \"ExpirationDate\": \"2021-11-10T00:00:00.000Z\",
        \"ExpirationInDays\": 365,
        \"ExpiredObjectDeleteMarker\": false,
        \"Filter\": {
          \"Predicate\": {
            \"Operands\": [
              {
                \"Prefix\": \"tmp/\",
                \"Type\": \"LifecyclePrefixPredicate\"
              },
              {
                \"Tag\": {
                  \"Key\": \"ArchiveAge\",
                  \"Value\": \"9m\"
                },
                \"Type\": \"LifecycleTagPredicate\"
              }
            ],
            \"Type\": \"LifecycleAndOperator\"
          }
        }
      }
    ]
  }
}
```

```

    },
    "ID": "Move rotated logs to Glacier",
    "NoncurrentVersionExpirationInDays": -1,
    "NoncurrentVersionTransitions": [
      {
        "Days": 2,
        "StorageClass": "GLACIER"
      }
    ],
    "Prefix": "rotated/",
    "Status": "Enabled",
    "Transitions": [
      {
        "Date": "2020-11-10T00:00:00.000Z",
        "Days": 100,
        "StorageClass": "GLACIER"
      }
    ]
  }
]
},
"BucketLoggingConfiguration": {
  "DestinationBucketName": "s3serversideloggingbucket-123456789012",
  "LogFilePrefix": "buckettestreadwrite23435/"
},
"BucketName": "amzn-s3-demo-bucket",
"BucketNotificationConfiguration": {
  "Configurations": [{
    "Destination": "arn:aws:lambda:us-east-1:123456789012:function:s3_public_write",
    "Events": [
      "s3:ObjectCreated:Put"
    ]
  }],
  "Filter": {
    "S3KeyFilter": {
      "FilterRules": [
        {
          "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.PREFIX",
          "Value": "pre"
        },
        {
          "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.SUFFIX",
          "Value": "suf"
        }
      ]
    }
  }
]

```

```

    }
  },
  "Type": "LambdaConfiguration"
}]
},
"BucketVersioningConfiguration": {
  "IsMfaDeleteEnabled": true,
  "Status": "Off"
},
"BucketWebsiteConfiguration": {
  "ErrorDocument": "error.html",
  "IndexDocumentSuffix": "index.html",
  "RedirectAllRequestsTo": {
    "HostName": "example.com",
    "Protocol": "http"
  },
  "RoutingRules": [{
    "Condition": {
      "HttpErrorCodeReturnedEquals": "Redirected",
      "KeyPrefixEquals": "index"
    },
    "Redirect": {
      "HostName": "example.com",
      "HttpRedirectCode": "401",
      "Protocol": "HTTP",
      "ReplaceKeyPrefixWith": "string",
      "ReplaceKeyWith": "string"
    }
  }]
},
"CreatedAt": "2007-11-30T01:46:56.000Z",
"ObjectLockConfiguration": {
  "ObjectLockEnabled": "Enabled",
  "Rule": {
    "DefaultRetention": {
      "Days": null,
      "Mode": "GOVERNANCE",
      "Years": 12
    },
  },
},
"OwnerId": "AIDACKCEVSQ6C2EXAMPLE",
"OwnerName": "s3bucketowner",
"PublicAccessBlockConfiguration": {

```

```

    "BlockPublicAcls": true,
    "BlockPublicPolicy": true,
    "IgnorePublicAcls": true,
    "RestrictPublicBuckets": true,
  },
  "ServerSideEncryptionConfiguration": {
    "Rules": [
      {
        "ApplyServerSideEncryptionByDefault": {
          "SSEAlgorithm": "AES256",
          "KMSMasterKeyID": "12345678-abcd-abcd-abcd-123456789012"
        }
      }
    ]
  }
}

```

AwsS3Object

Das `AwsS3Object` Objekt stellt Informationen über ein Amazon S3 S3-Objekt bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsS3Object` Objekt. Beschreibungen der `AwsS3Object` Attribute finden Sie unter [awSS3 ObjectDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsS3Object": {
  "ContentType": "text/html",
  "ETag": "\"30a6ec7e1a9ad79c203d05a589c8b400\"",
  "LastModified": "2012-04-23T18:25:43.511Z",
  "ServerSideEncryption": "aws:kms",
  "SSEKMSKeyId": "arn:aws:kms:us-west-2:123456789012:key/4dff8393-e225-4793-a9a0-608ec069e5a7",
  "VersionId": "ws310urg00jH_HH1lIxPE35P.MELYaYh"
}

```

AwsSageMakerRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsSageMaker` Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsSageMakerNotebookInstance

Das `AwsSageMakerNotebookInstance` Objekt stellt Informationen über eine Amazon SageMaker AI-Notebook-Instance bereit, bei der es sich um eine Recheninstanz für maschinelles Lernen handelt, auf der die Jupyter Notebook App ausgeführt wird.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt.

AwsSageMakerNotebookInstance Beschreibungen der `AwsSageMakerNotebookInstance` Attribute finden Sie [AwsSageMakerNotebookInstanceDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsSageMakerNotebookInstance": {
  "DirectInternetAccess": "Disabled",
  "InstanceMetadataServiceConfiguration": {
    "MinimumInstanceMetadataServiceVersion": "1",
  },
  "InstanceType": "ml.t2.medium",
  "LastModifiedTime": "2022-09-09 22:48:32.012000+00:00",
  "NetworkInterfaceId": "eni-06c09ac2541a1bed3",
  "NotebookInstanceArn": "arn:aws:sagemaker:us-east-1:001098605940:notebook-instance/sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm",
  "NotebookInstanceName":
  "SagemakerNotebookInstanceRootAccessDisabledComplia-8MYjcyofZiXm",
  "NotebookInstanceStatus": "InService",
  "PlatformIdentifier": "notebook-all-v1",
  "RoleArn": "arn:aws:iam::001098605940:role/sechub-SageMaker-1-scenar-SageMakerCustomExecution-1R0X32HGC38IW",
  "RootAccess": "Disabled",
  "SecurityGroups": [
    "sg-06b347359ab068745"
  ],
  "SubnetId": "subnet-02c0deea5fa64578e",
  "Url":
  "sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm.notebook.us-east-1.sagemaker.aws",
  "VolumeSizeInGB": 5
}
```

AwsSecretsManagerRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für AwsSecretsManager Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter. [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsSecretsManagerSecret

Das AwsSecretsManagerSecret Objekt enthält Details zu einem Secrets Manager Manager-Geheimnis.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das AwsSecretsManagerSecret Objekt. Beschreibungen der AwsSecretsManagerSecret Attribute finden Sie [AwsSecretsManagerSecretDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsSecretsManagerSecret": {
  "RotationRules": {
    "AutomaticallyAfterDays": 30
  },
  "RotationOccurredWithinFrequency": true,
  "KmsKeyId": "kmsKeyId",
  "RotationEnabled": true,
  "RotationLambdaArn": "arn:aws:lambda:us-west-2:777788889999:function:MyTestRotationLambda",
  "Deleted": false,
  "Name": "MyTestDatabaseSecret",
  "Description": "My test database secret"
}
```

AwsSnsRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für AwsSns Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter. [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsSnsTopic

Das `AwsSnsTopic` Objekt enthält Details zu einem Thema von Amazon Simple Notification Service.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsSnsTopic` Objekt. Beschreibungen der `AwsSnsTopic` Attribute finden Sie [AwsSnsTopicDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsSnsTopic": {
  "ApplicationSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
ApplicationSuccessFeedbackRoleArn",
  "FirehoseFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseFailureFeedbackRoleArn",
  "FirehoseSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseSuccessFeedbackRoleArn",
  "HttpFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpFailureFeedbackRoleArn",
  "HttpSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpSuccessFeedbackRoleArn",
  "KmsMasterKeyId": "alias/ExampleAlias",
  "Owner": "123456789012",
  "SqsFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsFailureFeedbackRoleArn",
  "SqsSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsSuccessFeedbackRoleArn",
  "Subscription": {
    "Endpoint": "http://sampleendpoint.com",
    "Protocol": "http"
  },
  "TopicName": "SampleTopic"
}
```

AwsSqsRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsSqs` Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsSqsQueue

Das `AwsSqsQueue` Objekt enthält Informationen über eine Amazon Simple Queue Service-Warteschlange.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsSqsQueue` Objekt. Beschreibungen der `AwsSqsQueue` Attribute finden Sie [AwsSqsQueueDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsSqsQueue": {
  "DeadLetterTargetArn": "arn:aws:sqs:us-west-2:123456789012:queue/target",
  "KmsDataKeyReusePeriodSeconds": 60,,
  "KmsMasterKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
  "QueueName": "sample-queue"
}
```

AwsSsmRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für `AwsSsm` Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsSsmPatchCompliance

Das `AwsSsmPatchCompliance` Objekt stellt Informationen über den Status eines Patches auf einer Instanz bereit, basierend auf der Patch-Baseline, die zum Patchen der Instanz verwendet wurde.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsSsmPatchCompliance` Objekt. Beschreibungen der `AwsSsmPatchCompliance` Attribute finden Sie [AwsSsmPatchComplianceDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsSsmPatchCompliance": {
  "Patch": {
    "ComplianceSummary": {
      "ComplianceType": "Patch",
```

```

    "CompliantCriticalCount": 0,
    "CompliantHighCount": 0,
    "CompliantInformationalCount": 0,
    "CompliantLowCount": 0,
    "CompliantMediumCount": 0,
    "CompliantUnspecifiedCount": 461,
    "ExecutionType": "Command",
    "NonCompliantCriticalCount": 0,
    "NonCompliantHighCount": 0,
    "NonCompliantInformationalCount": 0,
    "NonCompliantLowCount": 0,
    "NonCompliantMediumCount": 0,
    "NonCompliantUnspecifiedCount": 0,
    "OverallSeverity": "UNSPECIFIED",
    "PatchBaselineId": "pb-0c5b2769ef7cbe587",
    "PatchGroup": "ExamplePatchGroup",
    "Status": "COMPLIANT"
  }
}
}

```

AwsStepFunctionsRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für AwsStepFunctions Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter. [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsStepFunctionStateMachine

Das AwsStepFunctionStateMachine Objekt stellt Informationen über eine AWS Step Functions Zustandsmaschine bereit. Dabei handelt es sich um einen Workflow, der aus einer Reihe von ereignisgesteuerten Schritten besteht.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt.

AwsStepFunctionStateMachine Beschreibungen der AwsStepFunctionStateMachine Attribute finden Sie [AwsStepFunctionStateMachine](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsStepFunctionStateMachine": {

```

```

    "StateMachineArn": "arn:aws:states:us-east-1:123456789012:stateMachine:StepFunctionsLogDisableNonCompliantResource-fQLujTeXvwsb",
    "Name": "StepFunctionsLogDisableNonCompliantResource-fQLujTeXvwsb",
    "Status": "ACTIVE",
    "RoleArn": "arn:aws:iam::123456789012:role/teststepfunc-StatesExecutionRole-1PNM71RV01UKT",
    "Type": "STANDARD",
    "LoggingConfiguration": {
        "Level": "OFF",
        "IncludeExecutionData": false
    },
    "TracingConfiguration": {
        "Enabled": false
    }
}

```

AwsWafRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für AwsWaf Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsWafRateBasedRule

Das `AwsWafRateBasedRule` Objekt enthält Details zu einer AWS WAF ratenbasierten Regel für globale Ressourcen. Eine AWS WAF ratenbasierte Regel bietet Einstellungen, mit denen angegeben wird, wann eine Anfrage zugelassen, blockiert oder gezählt werden soll. Ratenbasierte Regeln beinhalten die Anzahl der Anfragen, die über einen bestimmten Zeitraum eingehen.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt.

`AwsWafRateBasedRule` Beschreibungen der `AwsWafRateBasedRule` Attribute finden Sie [AwsWafRateBasedRuleDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsWafRateBasedRule":{
    "MatchPredicates" : [{
        "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
        "Negated" : "True",
        "Type" : "IPMatch" ,

```

```

    }],
    "MetricName" : "MetricName",
    "Name" : "Test",
    "RateKey" : "IP",
    "RateLimit" : 235000,
    "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
  }

```

AwsWafRegionalRateBasedRule

Das `AwsWafRegionalRateBasedRule` Objekt enthält Details zu einer ratenbasierten Regel für regionale Ressourcen. Eine ratenbasierte Regel bietet Einstellungen, mit denen angegeben wird, wann eine Anfrage zugelassen, blockiert oder gezählt werden soll. Ratenbasierte Regeln beinhalten die Anzahl der Anfragen, die über einen bestimmten Zeitraum eingehen.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt.

Beschreibungen der `AwsWafRegionalRateBasedRule` Attribute finden Sie [AWSWafRegionalRateBasedRuleDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```

"AwsWafRegionalRateBasedRule":{
  "MatchPredicates" : [{
    "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
    "Negated" : "True",
    "Type" : "IPMatch" ,
  }],
  "MetricName" : "MetricName",
  "Name" : "Test",
  "RateKey" : "IP",
  "RateLimit" : 235000,
  "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
}

```

AwsWafRegionalRule

Das `AwsWafRegionalRule` Objekt enthält Details zu einer AWS WAF regionalen Regel. Diese Regel identifiziert die Webanfragen, die Sie zulassen, blockieren oder zählen möchten.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsWafRegionalRule` Objekt. Beschreibungen der `AwsWafRegionalRule` Attribute finden Sie [AWSWafRegionalRuleDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsWafRegionalRule": {
  "MetricName": "SampleWAF_Rule__Metric_1",
  "Name": "bb-waf-regional-rule-not-empty-conditions-compliant",
  "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de95fe",
  "PredicateList": [{
    "DataId": "127d9346-e607-4e93-9286-c1296fb5445a",
    "Negated": false,
    "Type": "GeoMatch"
  }]
}
```

AwsWafRegionalRuleGroup

Das `AwsWafRegionalRuleGroup` Objekt enthält Details zu einer AWS WAF regionalen Regelgruppe. Eine Regelgruppe ist eine Sammlung vordefinierter Regeln, die Sie einer Web-Zugriffskontrollliste (Web-ACL) hinzufügen.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsWafRegionalRuleGroup` Objekt. Beschreibungen der `AwsWafRegionalRuleGroup` Attribute finden Sie [AwsWafRegionalRuleGroupDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsWafRegionalRuleGroup": {
  "MetricName": "SampleWAF_Metric_1",
  "Name": "bb-WAFClassicRuleGroupWithRuleCompliant",
  "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
  "Rules": [{
    "Action": {
      "Type": "ALLOW"
    }
  ]},
  "Priority": 1,
  "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
  "Type": "REGULAR"
}
```


AwsWafRegionalWebAcl

`AwsWafRegionalWebAcl` enthält Einzelheiten zu einer AWS WAF regionalen Web-Zugriffskontrollliste (Web Access Control List, Web-ACL). Eine Web-ACL enthält die Regeln, die die Anfragen identifizieren, die Sie zulassen, blockieren oder zählen möchten.

Im Folgenden finden Sie ein Beispiel für einen `AwsWafRegionalWebAcl` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsApiGatewayV2Stage` Attribute finden Sie [AwsWafRegionalWebAclDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsWafRegionalWebAcl": {
  "DefaultAction": "ALLOW",
  "MetricName": "web-regional-webacl-metric-1",
  "Name": "WebACL_123",
  "RulesList": [
    {
      "Action": {
        "Type": "Block"
      },
      "Priority": 3,
      "RuleId": "24445857-852b-4d47-bd9c-61f05e4d223c",
      "Type": "REGULAR",
      "ExcludedRules": [
        {
          "ExclusionType": "Exclusion",
          "RuleId": "Rule_id_1"
        }
      ],
      "OverrideAction": {
        "Type": "OVERRIDE"
      }
    }
  ],
  "WebAclId": "443c76f4-2e72-4c89-a2ee-389d501c1f67"
}
```

AwsWafRule

`AwsWafRule` stellt Informationen zu einer AWS WAF Regel bereit. Eine AWS WAF Regel identifiziert die Webanfragen, die Sie zulassen, blockieren oder zählen möchten.

Im Folgenden finden Sie ein Beispiel für einen `AwsWafRule` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsApiGatewayV2Stage` Attribute finden Sie [AwsWafRuleDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsWafRule": {
  "MetricName": "AwsWafRule_Metric_1",
  "Name": "AwsWafRule_Name_1",
  "PredicateList": [{
    "DataId": "cdd225da-32cf-4773-1dc2-3bca3ed9c19c",
    "Negated": false,
    "Type": "GeoMatch"
  }],
  "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de953e"
}
```

AwsWafRuleGroup

`AwsWafRuleGroup` stellt Informationen zu einer AWS WAF Regelgruppe bereit. Eine AWS WAF Regelgruppe ist eine Sammlung vordefinierter Regeln, die Sie einer Web-Zugriffskontrollliste (Web-ACL) hinzufügen.

Im Folgenden finden Sie ein Beispiel für einen `AwsWafRuleGroup` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsApiGatewayV2Stage` Attribute finden Sie [AwsWafRuleGroupDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsWafRuleGroup": {
  "MetricName": "SampleWAF_Metric_1",
  "Name": "bb-WAFRuleGroupWithRuleCompliant",
  "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
  "Rules": [{
    "Action": {
      "Type": "ALLOW",
    },
    "Priority": 1,
    "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
    "Type": "REGULAR"
  }]
}
```

AwsWafv2RuleGroup

Das `AwsWafv2RuleGroup` Objekt enthält Details zu einer AWS WAF V2-Regelgruppe.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsWafv2RuleGroup` Objekt. Beschreibungen der `AwsWafv2RuleGroup` Attribute finden Sie unter [AwsWafv2RuleGroupDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsWafv2RuleGroup": {
  "Arn": "arn:aws:wafv2:us-east-1:123456789012:global/rulegroup/wafv2rulegroupasff/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Capacity": 1000,
  "Description": "Resource for ASFF",
  "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Name": "wafv2rulegroupasff",
  "Rules": [{
    "Action": {
      "Allow": {
        "CustomRequestHandling": {
          "InsertHeaders": [
            {
              "Name": "AllowActionHeader1Name",
              "Value": "AllowActionHeader1Value"
            },
            {
              "Name": "AllowActionHeader2Name",
              "Value": "AllowActionHeader2Value"
            }
          ]
        }
      }
    },
    "Name": "RuleOne",
    "Priority": 1,
    "VisibilityConfig": {
      "CloudWatchMetricsEnabled": true,
      "MetricName": "rulegroupasff",
      "SampledRequestsEnabled": false
    }
  }],
  "VisibilityConfig": {
    "CloudWatchMetricsEnabled": true,
```

```
    "MetricName": "rulegroupasff",
    "SampledRequestsEnabled": false
  }
}
```

AwsWafWebAcl

Das `AwsWafWebAcl` Objekt enthält Details zu einer AWS WAF Web-ACL.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsWafWebAcl` Objekt. Beschreibungen der `AwsWafWebAcl` Attribute finden Sie [AwsWafWebAclDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsWafWebAcl": {
  "DefaultAction": "ALLOW",
  "Name": "MyWafAcl",
  "Rules": [
    {
      "Action": {
        "Type": "ALLOW"
      },
      "ExcludedRules": [
        {
          "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98"
        }
      ],
      "OverrideAction": {
        "Type": "NONE"
      },
      "Priority": 1,
      "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98",
      "Type": "REGULAR"
    }
  ],
  "WebAclId": "waf-1234567890"
}
```

AwsWafv2WebAcl

Das `AwsWafv2WebAcl` Objekt enthält Details zu einer AWS WAF V2-Web-ACL.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsWafv2WebAcl` Objekt. Beschreibungen der `AwsWafv2WebAcl` Attribute finden Sie unter [AwsWafv2 WebAclDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsWafv2WebAcl": {
  "Arn": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/WebACL-RoaD4QexqSxG/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Capacity": 1326,
  "CaptchaConfig": {
    "ImmunityTimeProperty": {
      "ImmunityTime": 500
    }
  },
  "DefaultAction": {
    "Block": {}
  },
  "Description": "Web ACL for JsonBody testing",
  "ManagedbyFirewallManager": false,
  "Name": "WebACL-RoaD4QexqSxG",
  "Rules": [{
    "Action": {
      "RuleAction": {
        "Block": {}
      }
    },
    "Name": "TestJsonBodyRule",
    "Priority": 1,
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "JsonBodyMatchMetric"
    }
  }],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "TestingJsonBodyMetric"
  }
}
```

AwsXrayRessourcen in ASFF

Im Folgenden finden Sie Beispiele für die ASFF-Syntax (AWS Security Finding Format) für AwsXray Ressourcen.

AWS Security Hub normalisiert Ergebnisse aus verschiedenen Quellen in ASFF.

Hintergrundinformationen zu ASFF finden Sie unter [AWS Format für Sicherheitssuche \(ASFF\)](#)

AwsXrayEncryptionConfig

Das AwsXrayEncryptionConfig Objekt enthält Informationen zur Verschlüsselungskonfiguration für AWS X-Ray.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das AwsXrayEncryptionConfig Objekt. Beschreibungen der AwsXrayEncryptionConfig Attribute finden Sie [AwsXrayEncryptionConfigDetails](#) in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsXRayEncryptionConfig":{
  "KeyId": "arn:aws:kms:us-east-2:222222222222:key/example-key",
  "Status": "UPDATING",
  "Type": "KMS"
}
```

ContainerASFF-Objekt

Das folgende Beispiel zeigt die ASFF-Syntax (AWS Security Finding Format) für das Container Objekt. Beschreibungen der Container Attribute finden Sie [ContainerDetails](#) in der AWS Security Hub API-Referenz. Hintergrundinformationen zu ASFF finden Sie unter [AWS Format für Sicherheitssuche \(ASFF\)](#).

Beispiel

```
"Container": {
  "ContainerRuntime": "docker",
  "ImageId": "image12",
  "ImageName": "11111111/
knotejs@sha256:372131c9fef111111111111111115f4ed3ea5f9dce4dc3bd34ce21846588a3",
  "LaunchedAt": "2018-09-29T01:25:54Z",
  "Name": "knote",
```

```
"Privileged": true,
"VolumeMounts": [{
  "Name": "vol-03909e9",
  "MountPath": "/mnt/etc"
}]
}
```

OtherASFF-Objekt

Das folgende Beispiel zeigt die ASFF-Syntax (AWS Security Finding Format) für das `Other` Objekt. Hintergrundinformationen zu ASFF finden Sie unter [AWS Format für Sicherheitssuche \(ASFF\)](#).

Mit dem `Other` Objekt können Sie benutzerdefinierte Felder und Werte angeben. Sie verwenden das `Other` Objekt in den folgenden Fällen.

- Der Ressourcentyp hat kein entsprechendes `Details` Objekt. Um Details für die Ressource bereitzustellen, verwenden Sie das `Other` Objekt.
- Das `Details` Objekt für den Ressourcentyp enthält nicht alle Attribute, die Sie auffüllen möchten. Verwenden Sie in diesem Fall das `Details` Objekt für den Ressourcentyp, um die verfügbaren Attribute aufzufüllen. Verwenden Sie das `Other` Objekt, um die Attribute aufzufüllen, die sich nicht im typspezifischen Objekt befinden.
- Der Ressourcentyp gehört nicht zu den angegebenen Typen. In diesem Fall legen Sie den Wert `Resource.Type` auf fest und verwenden das `Other` Objekt, um die Details aufzufüllen.

Typ: Karte mit bis zu 50 Schlüssel-Wert-Paaren

Jedes Schlüssel-Wert-Paar muss die folgenden Anforderungen erfüllen.

- Der Schlüssel muss weniger als 128 Zeichen enthalten.
- Der Wert muss weniger als 1.024 Zeichen enthalten.

Einblicke in Security Hub CSPM anzeigen

In AWS Security Hub Cloud Security Posture Management (CSPM) ist ein Insight eine Sammlung verwandter Erkenntnisse. Ein Einblick kann einen bestimmten Sicherheitsbereich identifizieren, der Aufmerksamkeit und Intervention erfordert. Ein Einblick könnte beispielsweise auf EC2 Fälle hinweisen, bei denen festgestellt wurde, dass schlechte Sicherheitspraktiken aufgedeckt wurden. Ein Insight bringt Ergebnisse von verschiedenen Ergebnis-Anbietern zusammen.

Jedes Insight wird von einer Gruppe durch Anweisung und optionale Filter definiert. Die Gruppe nach Anweisung gibt an, wie die übereinstimmenden Ergebnisse gruppiert werden sollen, und identifiziert den Elementtyp, für den das Insight gilt. Wenn beispielsweise ein Insight nach Ressourcenbezeichner gruppiert ist, erstellt das Insight eine Liste von Ressourcenbezeichnern. Die optionalen Filter identifizieren die passenden Ergebnisse für den Einblick. Beispielsweise möchten Sie möglicherweise nur Ergebnisse von bestimmten Anbietern oder Ergebnisse sehen, die mit bestimmten Ressourcentypen verknüpft sind.

Security Hub CSPM bietet mehrere integrierte verwaltete Einblicke. Sie können verwaltete Erkenntnisse nicht ändern oder löschen. Um Sicherheitsprobleme nachzuverfolgen, die für Ihre AWS Umgebung und Nutzung spezifisch sind, können Sie benutzerdefinierte Einblicke erstellen.

Auf der Insights-Seite der AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole wird die Liste der verfügbaren Erkenntnisse angezeigt.

Standardmäßig werden in der Liste sowohl verwaltete als auch benutzerdefinierte Erkenntnisse angezeigt. Um die Insight-Liste nach dem Insight-Typ zu filtern, wählen Sie den Insight-Typ aus dem Drop-down-Menü neben dem Filterfeld aus.

- Um alle verfügbaren Erkenntnisse anzuzeigen, wählen Sie Alle Erkenntnisse aus. Dies ist die Standardoption.
- Um nur verwaltete Einblicke anzuzeigen, wählen Sie Security Hub CSPM managed insights.
- Um nur benutzerdefinierte Insights anzuzeigen, wählen Sie Custom Insights.

Sie können die Insight-Liste auch nach dem Namen des Insights filtern. Geben Sie dazu in das Filterfeld den Text ein, der zum Filtern der Liste verwendet werden soll. Der Filter unterscheidet nicht zwischen Groß- und Kleinschreibung. Der Filter sucht nach Erkenntnissen, die den Text an einer beliebigen Stelle im Insight-Namen enthalten.

Ein Insight gibt nur dann Ergebnisse zurück, wenn Sie Integrationen oder Standards aktiviert haben, die zu passenden Ergebnissen führen. Zum Beispiel der verwaltete Einblick 29. Die Liste der Ressourcen mit der höchsten Anzahl fehlgeschlagener CIS-Prüfungen gibt nur dann Ergebnisse zurück, wenn Sie eine Version des Benchmark-Standards der Center for Internet Security (CIS) AWS Foundations aktivieren.

Überprüfung und Umsetzung von Erkenntnissen in Security Hub CSPM

Für jeden Einblick ermittelt AWS Security Hub Cloud Security Posture Management (CSPM) zunächst die Ergebnisse, die den Filterkriterien entsprechen, und verwendet dann das Gruppierungsattribut, um die übereinstimmenden Ergebnisse zu gruppieren.

Auf der Insights-Seite in der Konsole können Sie die Ergebnisse und Ergebnisse einsehen und entsprechende Maßnahmen ergreifen.

Wenn Sie die regionsübergreifende Aggregation aktivieren, enthalten die Ergebnisse für verwaltete Einblicke (wenn Sie in der Aggregationsregion angemeldet sind) Ergebnisse aus der Aggregationsregion und den verknüpften Regionen. Wenn die Erkenntnisse nicht nach Region gefiltert werden, enthalten die Ergebnisse für benutzerdefinierte Einblicke auch Ergebnisse aus der Aggregationsregion und verknüpften Regionen (wenn Sie bei der Aggregationsregion angemeldet sind). In anderen Regionen beziehen sich die Insight-Ergebnisse nur auf diese Region.

Informationen zur Konfiguration der regionsübergreifenden Aggregation finden Sie unter [Aggregation von CSPM-Daten über Regionen hinweg](#)

Insight-Ergebnisse anzeigen und entsprechende Maßnahmen ergreifen

Die Insight-Ergebnisse bestehen aus einer gruppierten Liste der Ergebnisse für den Insight. Wenn die Erkenntnisse beispielsweise nach Ressourcen-Identifikatoren gruppiert sind, dann sind die Insight-Ergebnisse die Liste der Ressourcen-Identifikatoren. Jedes Element in der Ergebnisliste gibt die Anzahl der übereinstimmenden Ergebnisse für dieses Element an.

Wenn die Ergebnisse nach Ressourcen-ID oder Ressourcentyp gruppiert sind, umfassen die Ergebnisse alle Ressourcen, die in den entsprechenden Ergebnissen enthalten sind. Dazu gehören Ressourcen, deren Typ sich von dem in den Filterkriterien angegebenen Ressourcentyp unterscheidet. Ein Insight identifiziert beispielsweise Ergebnisse, die mit S3-Buckets verknüpft sind. Wenn ein übereinstimmendes Ergebnis sowohl eine S3-Bucket-Ressource als auch eine IAM-Zugriffsschlüsselressource enthält, umfassen die Insight-Ergebnisse beide Ressourcen.

Auf der Security Hub CSPM-Konsole ist die Ergebnisliste von den Ergebnissen mit den meisten bis zu den wenigsten übereinstimmenden Ergebnissen sortiert. Security Hub CSPM kann nur 100 Ergebnisse anzeigen. Wenn es mehr als 100 Gruppierungswerte gibt, werden nur die ersten 100 angezeigt.

Zusätzlich zur Ergebnisliste wird in den Insight-Ergebnissen eine Reihe von Diagrammen angezeigt, die die Anzahl der übereinstimmenden Ergebnisse für die folgenden Attribute zusammenfassen.

- Bezeichnung des Schweregrads — Anzahl der Ergebnisse für jeden Schweregrad
- AWS-Konto ID — Die fünf wichtigsten Konten IDs für die übereinstimmenden Ergebnisse
- Ressourcentyp — Die fünf wichtigsten Ressourcentypen für die passenden Ergebnisse
- Ressourcen-ID — Die fünf wichtigsten Ressourcen IDs für die passenden Ergebnisse
- Produktname — Die fünf besten Anbieter für die Suche nach den passenden Ergebnissen

Wenn Sie benutzerdefinierte Aktionen konfiguriert haben, können Sie ausgewählte Ergebnisse an eine benutzerdefinierte Aktion senden. Die Aktion muss mit einer CloudWatch Amazon-Regel für den Security Hub Insight Results Ereignistyp verknüpft sein. Weitere Informationen finden Sie unter [the section called “Automatisierte Reaktion und Problembehebung”](#). Wenn Sie keine benutzerdefinierten Aktionen konfiguriert haben, ist das Aktionsmenü deaktiviert.

Security Hub CSPM console

So können Sie Insight-Ergebnisse anzeigen und entsprechende Maßnahmen ergreifen (Konsole)

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Insights aus.
3. Um die Liste der Insight-Ergebnisse anzuzeigen, wählen Sie den Insight-Namen aus.
4. Wählen Sie das Kontrollkästchen für jedes Ergebnis, das an die benutzerdefinierte Aktion gesendet werden soll.
5. Wählen Sie im Menü Actions (Aktionen) die benutzerdefinierte Aktion aus.

Security Hub CSPM API, AWS CLI

Um Insight-Ergebnisse einzusehen und entsprechende Maßnahmen zu ergreifen (API,) AWS CLI

Verwenden Sie den [GetInsightResults](#) Betrieb der Security Hub CSPM-API, um Insight-Ergebnisse anzuzeigen. Wenn Sie den verwenden AWS CLI, führen Sie den [get-insight-results](#) Befehl aus.

Um die Erkenntnisse zu identifizieren, für die Ergebnisse zurückgegeben werden sollen, benötigen Sie den Insight-ARN. Verwenden Sie die [GetInsights](#) API-Operation oder den [get-insight-results](#) Befehl, um die Erkenntnisse ARNs für benutzerdefinierte Erkenntnisse zu erhalten.

Im folgenden Beispiel werden die Ergebnisse für den angegebenen Einblick abgerufen. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub get-insight-results --insight-arn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Informationen zum programmgesteuerten Erstellen benutzerdefinierter Aktionen finden Sie unter [Verwenden von benutzerdefinierten Aktionen zum Senden von Ergebnissen und Erkenntnisergebnissen an EventBridge](#)

Ergebnisse von Insight-Ergebnissen anzeigen und entsprechende Maßnahmen ergreifen (Konsole)

In einer Insight-Ergebnisliste auf der Security Hub CSPM-Konsole können Sie die Ergebnisliste für jedes Ergebnis anzeigen.

Um Insight-Ergebnisse anzuzeigen und entsprechende Maßnahmen zu ergreifen (Konsole)

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Insights aus.
3. Um die Liste der Insight-Ergebnisse anzuzeigen, wählen Sie den Insight-Namen aus.
4. Um die Liste der Ergebnisse für ein Insight-Ergebnis anzuzeigen, wählen Sie das Element aus der Ergebnisliste aus. Die Ergebnisliste zeigt die aktiven Ergebnisse für das ausgewählte Insight-Ergebnis mit dem Workflow-Status NEW oder NOTIFIED.

Von der Ergebnisliste aus können Sie die folgenden Aktionen ausführen:

- [Ergebnisse im Security Hub CSPM filtern](#)
- [Details und Verlauf der Ergebnisse überprüfen](#)
- [Den Workflow-Status von Ergebnissen in Security Hub CSPM festlegen](#)
- [Ergebnisse an eine benutzerdefinierte Security Hub CSPM-Aktion senden](#)

Verwaltete Einblicke in Security Hub CSPM

AWS Security Hub Cloud Security Posture Management (CSPM) bietet verschiedene verwaltete Einblicke.

Sie können von Security Hub CSPM verwaltete Einblicke nicht bearbeiten oder löschen. Sie können die [Insight-Ergebnisse und -Resultate einsehen und Maßnahmen ergreifen](#). Sie können auch [einen verwalteten Insight als Grundlage für einen neuen benutzerdefinierten Insight verwenden](#).

Wie bei allen Insights gibt ein verwalteter Insight nur Ergebnisse zurück, wenn Sie Produktintegrationen oder Sicherheitsstandards aktiviert haben, die zu passenden Ergebnissen führen können.

Bei Erkenntnissen, die nach Ressourcen-IDs gruppiert sind, enthalten die Ergebnisse die Identifikatoren aller Ressourcen in den entsprechenden Ergebnissen. Dazu gehören Ressourcen, deren Typ sich von dem in den Filterkriterien angegebenen Ressourcentyp unterscheidet. Insight 2 in der folgenden Liste identifiziert beispielsweise Ergebnisse, die mit Amazon S3 S3-Buckets verknüpft sind. Wenn ein übereinstimmendes Ergebnis sowohl eine S3-Bucket-Ressource als auch eine IAM-Zugriffsschlüsselressource enthält, umfassen die Insight-Ergebnisse beide Ressourcen.

Security Hub CSPM bietet derzeit die folgenden verwalteten Einblicke:

1. AWS Ressourcen mit den meisten Ergebnissen

ARN: `arn:aws:securityhub:::insight/securityhub/default/1`

Gruppiert nach: Ressourcen-ID

Filter finden:

- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

2. S3-Buckets mit öffentlichen Lese- oder Schreibberechtigungen

ARN: `arn:aws:securityhub:::insight/securityhub/default/10`

Gruppieren nach: Ressourcen-ID

Filter finden:

- Typ beginnt mit Effects/Data Exposure
- Ressourcentyp ist AwsS3Bucket
- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

3. AMIs die die meisten Erkenntnisse generieren

ARN: `arn:aws:securityhub:::insight/securityhub/default/3`

Gruppieren nach: EC2 Instanz-Image-ID

Filter finden:

- Ressourcentyp ist AwsEc2Instance
- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

4. EC2 Fälle, die an bekannten Taktiken, Techniken und Verfahren beteiligt sind (TTPs)

ARN: `arn:aws:securityhub:::insight/securityhub/default/14`

Gruppieren nach: Ressourcen-ID

Filter finden:

- Typ beginnt mit TTPs
- Ressourcentyp ist AwsEc2Instance
- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

5. AWS Principals mit verdächtiger Zugriffsschlüsselaktivität

ARN: `arn:aws:securityhub:::insight/securityhub/default/9`

Gruppieren nach: Prinzipalname des IAM-Zugriffsschlüssels

Filter finden:

- Ressourcentyp ist AwsIamAccessKey

- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

6. AWS Ressourcen und Instanzen, die die Sicherheitsstandards/Best Practices nicht erfüllen

ARN: `arn:aws:securityhub:::insight/securityhub/default/6`

Gruppert nach: Ressourcen-ID

Filter finden:

- Typ ist Software and Configuration Checks/Industry and Regulatory Standards/AWS Security Best Practices
- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

7. AWS Ressourcen im Zusammenhang mit potenzieller Datenexfiltration

ARN: `arn:aws:securityhub:::insight/securityhub/default/7`

Gruppert nach: Ressourcen-ID

Filter finden:

- Der Typ beginnt mit Effects/Data Exfiltration/
- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

8. AWS Ressourcen, die mit unberechtigtem Ressourcenverbrauch verbunden sind

ARN: `arn:aws:securityhub:::insight/securityhub/default/8`

Gruppert nach: Ressourcen-ID

Filter finden:

- Typ beginnt mit Effects/Resource Consumption
- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

9. S3-Buckets, die Sicherheitsstandards oder Best Practices nicht erfüllen

ARN: `arn:aws:securityhub:::insight/securityhub/default/11`

Gruppieren nach: Ressourcen-ID

Filter finden:

- Ressourcentyp ist AwsS3Bucket
- Typ ist Software and Configuration Checks/Industry and Regulatory Standards/AWS Security Best Practices
- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

10. S3-Buckets mit sensiblen Daten

ARN: `arn:aws:securityhub:::insight/securityhub/default/12`

Gruppieren nach: Ressourcen-ID

Filter finden:

- Ressourcentyp ist AwsS3Bucket
- Typ beginnt mit Sensitive Data Identifications/
- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

11. Anmeldeinformationen, die möglicherweise in falsche Hände geraten sind

ARN: `arn:aws:securityhub:::insight/securityhub/default/13`

Gruppieren nach: Ressourcen-ID

Filter finden:

- Typ beginnt mit Sensitive Data Identifications/Passwords/
- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

12. EC2 Instanzen, bei denen Sicherheitspatches für wichtige Sicherheitslücken fehlen

ARN: `arn:aws:securityhub:::insight/securityhub/default/16`

Gruppieren nach: Ressourcen-ID

Filter finden:

- Typ beginnt mit Software and Configuration Checks/Vulnerabilities/CVE
- Ressourcentyp ist AwsEc2Instance
- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

13. EC2 Fälle mit allgemein ungewöhnlichem Verhalten

ARN: `arn:aws:securityhub:::insight/securityhub/default/17`

Gruppiert nach: Ressourcen-ID

Filter finden:

- Typ beginnt mit Unusual Behaviors
- Ressourcentyp ist AwsEc2Instance
- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

14. EC2 Instanzen, deren Ports über das Internet zugänglich sind

ARN: `arn:aws:securityhub:::insight/securityhub/default/18`

Gruppiert nach: Ressourcen-ID

Filter finden:

- Typ beginnt mit Software and Configuration Checks/AWS Security Best Practices/Network Reachability
- Ressourcentyp ist AwsEc2Instance
- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

15. EC2 Instanzen, die die Sicherheitsstandards/Best Practices nicht erfüllen

ARN: `arn:aws:securityhub:::insight/securityhub/default/19`

Gruppiert nach: Ressourcen-ID

Filter finden:

- Typ beginnt mit einer der folgenden Möglichkeiten:
 - Software and Configuration Checks/Industry and Regulatory Standards/

- Software and Configuration Checks/AWS Security Best Practices
- Ressourcentyp ist AwsEc2Instance
- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

16. EC2 Instanzen, die für das Internet offen sind

ARN: `arn:aws:securityhub:::insight/securityhub/default/21`

Gruppiert nach: Ressourcen-ID

Filter finden:

- Typ beginnt mit Software and Configuration Checks/AWS Security Best Practices/Network Reachability
- Ressourcentyp ist AwsEc2Instance
- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

17. EC2 Fälle im Zusammenhang mit der Aufklärung von Gegnern

ARN: `arn:aws:securityhub:::insight/securityhub/default/22`

Gruppiert nach: Ressourcen-ID

Filter finden:

- Der Typ beginnt mit TTPs /Discovery/Recon
- Ressourcentyp ist AwsEc2Instance
- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

18. AWS Ressourcen, die mit Malware in Verbindung stehen

ARN: `arn:aws:securityhub:::insight/securityhub/default/23`

Gruppiert nach: Ressourcen-ID

Filter finden:

- Typ beginnt mit einer der folgenden Möglichkeiten:
 - Effects/Data Exfiltration/Trojan

- TTPs/Initial Access/Trojan
- TTPs/Command and Control/Backdoor
- TTPs/Command and Control/Trojan
- Software and Configuration Checks/Backdoor
- Unusual Behaviors/VM/Backdoor
- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

19. AWS Ressourcen im Zusammenhang mit Kryptowährungsproblemen

ARN: `arn:aws:securityhub:::insight/securityhub/default/24`

Gruppiert nach: Ressourcen-ID

Filter finden:

- Typ beginnt mit einer der folgenden Möglichkeiten:
 - Effects/Resource Consumption/Cryptocurrency
 - TTPs/Command and Control/CryptoCurrency
- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

20. AWS Ressourcen mit unbefugten Zugriffsversuchen

ARN: `arn:aws:securityhub:::insight/securityhub/default/25`

Gruppiert nach: Ressourcen-ID

Filter finden:

- Typ beginnt mit einer der folgenden Möglichkeiten:
 - TTPs/Command and Control/UnauthorizedAccess
 - TTPs/Initial Access/UnauthorizedAccess
 - Effects/Data Exfiltration/UnauthorizedAccess
 - Unusual Behaviors/User/UnauthorizedAccess
 - Effects/Resource Consumption/UnauthorizedAccess
- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

21. Bedrohungsinformationsindikatoren mit den meisten Treffern in der letzten Woche

ARN: `arn:aws:securityhub:::insight/securityhub/default/26`

Filter finden:

- Erstellt innerhalb der letzten 7 Tage

22. Top-Konten nach Anzahl der Ergebnisse

ARN: `arn:aws:securityhub:::insight/securityhub/default/27`

Gruppiert nach: AWS-Konto ID

Filter finden:

- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

23. Top-Produkte nach Anzahl der Ergebnisse

ARN: `arn:aws:securityhub:::insight/securityhub/default/28`

Gruppiert nach: Produktname

Filter finden:

- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

24. Schweregrad nach Anzahl der Ergebnisse

ARN: `arn:aws:securityhub:::insight/securityhub/default/29`

Gruppiert nach: Bezeichnung Schweregrad

Filter finden:

- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

25. Top S3-Buckets nach Anzahl der Ergebnisse

ARN: `arn:aws:securityhub:::insight/securityhub/default/30`

Gruppiert nach: Ressourcen-ID

Filter finden:

- Ressourcentyp ist AwsS3Bucket
- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

26. Häufigste EC2 Fälle nach Anzahl der Ergebnisse

ARN: `arn:aws:securityhub:::insight/securityhub/default/31`

Gruppiert nach: Ressourcen-ID

Filter finden:

- Ressourcentyp ist AwsEc2Instance
- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

27. AMIs Nach Anzahl der Ergebnisse am höchsten

ARN: `arn:aws:securityhub:::insight/securityhub/default/32`

Gruppiert nach: Image-ID der EC2 Instanz

Filter finden:

- Ressourcentyp ist AwsEc2Instance
- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

28. Top-IAM-Benutzer nach Anzahl der Ergebnisse

ARN: `arn:aws:securityhub:::insight/securityhub/default/33`

Gruppiert nach: IAM-Zugriffsschlüssel-ID

Filter finden:

- Ressourcentyp ist AwsIamAccessKey
- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

29. Top-Ressourcen nach Anzahl fehlgeschlagener CIS-Prüfungen

ARN: `arn:aws:securityhub:::insight/securityhub/default/34`

Gruppieren nach: Ressourcen-ID

Filter finden:

- Generator-ID beginnt mit `arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule`
- Aktualisiert am letzten Tag
- Compliance-Status ist FAILED
- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

30. Top-Integrationen nach Anzahl der Ergebnisse

ARN: `arn:aws:securityhub:::insight/securityhub/default/35`

Gruppieren nach: Produkt ARN

Filter finden:

- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

31. Ressourcen mit den am meisten fehlgeschlagenen Sicherheitsprüfungen

ARN: `arn:aws:securityhub:::insight/securityhub/default/36`

Gruppieren nach: Ressourcen-ID

Filter finden:

- Aktualisiert am letzten Tag
- Compliance-Status ist FAILED
- Datensatzstatus ist ACTIVE
- Workflow-Status ist NEW oder NOTIFIED

32. IAM-Benutzer mit verdächtigen Aktivitäten

ARN: `arn:aws:securityhub:::insight/securityhub/default/37`

Gruppieren nach: IAM-Benutzer

Filter finden:

- Ressourcentyp ist `AwsIamUser`
- Datensatzstatus ist `ACTIVE`
- Workflow-Status ist `NEW` oder `NOTIFIED`

33. Ressourcen mit den meisten AWS Health Ergebnissen

ARN: `arn:aws:securityhub:::insight/securityhub/default/38`

Gruppiert nach: Ressourcen-ID

Filter finden:

- `ProductName` ist gleich `Health`

34. Ressourcen mit den meisten AWS Config Ergebnissen

ARN: `arn:aws:securityhub:::insight/securityhub/default/39`

Gruppiert nach: Ressourcen-ID

Filter finden:

- `ProductName` ist gleich `Config`

35. Anwendungen mit den meisten Ergebnissen

ARN: `arn:aws:securityhub:::insight/securityhub/default/40`

Gruppiert nach: `ResourceApplicationArn`

Filter finden:

- `RecordState` ist gleich `ACTIVE`
- `Workflow.Status` ist gleich oder `NEW NOTIFIED`

Grundlegendes zu benutzerdefinierten Erkenntnissen in Security Hub CSPM

Zusätzlich zu den verwalteten Erkenntnissen von AWS Security Hub Cloud Security Posture Management (CSPM) können Sie benutzerdefinierte Einblicke in Security Hub CSPM erstellen, um Probleme zu verfolgen, die für Ihre Umgebung spezifisch sind. Mithilfe von benutzerdefinierten Erkenntnissen können Sie eine kuratierte Teilmenge von Problemen verfolgen.

Hier sind einige Beispiele für benutzerdefinierte Einblicke, deren Einrichtung nützlich sein kann:

- Wenn Sie ein Administratorkonto besitzen, können Sie einen benutzerdefinierten Einblick einrichten, um kritische und schwerwiegende Ergebnisse nachzuverfolgen, die sich auf Mitgliedskonten auswirken.
- Wenn Sie sich auf einen bestimmten [integrierten AWS Service](#) verlassen, können Sie einen benutzerdefinierten Einblick einrichten, um kritische und schwerwiegende Ergebnisse dieses Dienstes nachzuverfolgen.
- Wenn Sie sich auf die [Integration eines Drittanbieters](#) verlassen, können Sie einen benutzerdefinierten Einblick einrichten, um kritische und schwerwiegende Ergebnisse dieses integrierten Produkts nachzuverfolgen.

Sie können völlig neue benutzerdefinierte Insights erstellen oder von einem vorhandenen benutzerdefinierten oder verwalteten Insight ausgehen.

Jeder Einblick kann mit den folgenden Optionen konfiguriert werden:

- Gruppierungsattribut — Das Gruppierungsattribut bestimmt, welche Elemente in der Insight-Ergebnisliste angezeigt werden. Wenn das Gruppierungsattribut beispielsweise Produktname lautet, zeigen die Insight-Ergebnisse die Anzahl der Ergebnisse an, die jedem Ergebnisanbieter zugeordnet sind.
- Optionale Filter — Die Filter grenzen die passenden Ergebnisse für den Einblick ein.

Ein Ergebnis ist nur dann in den Insight-Ergebnissen enthalten, wenn es allen bereitgestellten Filtern entspricht. Wenn die Filter beispielsweise „Produktname ist GuardDuty“ und „Ressourcentyp istAwsS3Bucket“ lauten, müssen übereinstimmende Ergebnisse diesen beiden Kriterien entsprechen.

Security Hub CSPM wendet jedoch eine boolesche OR-Logik auf Filter an, die dasselbe Attribut, aber unterschiedliche Werte verwenden. Wenn die Filter beispielsweise „Produktname ist“ und GuardDuty „Produktname ist Amazon Inspector“ lauten, stimmt ein Ergebnis überein, wenn es entweder von Amazon GuardDuty oder Amazon Inspector generiert wurde.

Wenn Sie die Ressourcen-ID oder den Ressourcentyp als Gruppierungsattribut verwenden, umfassen die Insight-Ergebnisse alle Ressourcen, die in den passenden Ergebnissen enthalten sind. Die Liste ist nicht auf Ressourcen beschränkt, die einem Ressourcentypfilter entsprechen. Ein Insight identifiziert beispielsweise Ergebnisse, die mit S3-Buckets verknüpft sind, und gruppiert

diese Ergebnisse nach der Ressourcen-ID. Ein übereinstimmendes Ergebnis enthält sowohl eine S3-Bucket-Ressource als auch eine IAM-Zugriffsschlüsselressource. Die Insight-Ergebnisse umfassen beide Ressourcen.

Wenn Sie die [regionsübergreifende Aggregation](#) aktivieren und anschließend einen benutzerdefinierten Einblick erstellen, gilt der Einblick für den Abgleich von Ergebnissen in der Aggregationsregion und den verknüpften Regionen. Die Ausnahme ist, wenn Ihre Erkenntnisse einen Regionsfilter enthalten.

Einen benutzerdefinierten Einblick erstellen

In AWS Security Hub Cloud Security Posture Management (CSPM) können benutzerdefinierte Erkenntnisse verwendet werden, um bestimmte Ergebnisse zu sammeln und Probleme zu verfolgen, die nur in Ihrer Umgebung auftreten. Hintergrundinformationen zu benutzerdefinierten Erkenntnissen finden Sie unter [Grundlegendes zu benutzerdefinierten Erkenntnissen in Security Hub CSPM](#)

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um einen benutzerdefinierten Einblick in Security Hub CSPM zu erstellen

Security Hub CSPM console

Um einen benutzerdefinierten Einblick zu erstellen (Konsole)

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Insights aus.
3. Wählen Sie Create Insight (Insight erstellen) aus.
4. So wählen Sie das Gruppierungsattribut für den Insight aus:
 - a. Wählen Sie das Suchfeld, um die Filteroptionen anzuzeigen.
 - b. Wählen Sie Group by (Gruppieren nach).
 - c. Wählen Sie das Attribut aus, das verwendet werden soll, um die Ergebnisse zu gruppieren, die mit dieser Erkenntnis verknüpft sind.
 - d. Wählen Sie Anwenden aus.
5. Wählen Sie optional weitere Filter aus, die für diesen Einblick verwendet werden sollen. Definieren Sie für jeden Filter die Filterkriterien und wählen Sie dann Anwenden aus.
6. Wählen Sie Create Insight (Insight erstellen) aus.

7. Geben Sie einen Insight-Namen ein und wählen Sie dann Create Insight aus.

Security Hub CSPM API

Um einen benutzerdefinierten Einblick (API) zu erstellen

1. Verwenden Sie den [CreateInsight](#) Betrieb der Security Hub CSPM-API, um einen benutzerdefinierten Einblick zu erstellen. Wenn Sie den verwenden AWS CLI, führen Sie den [create-insight](#) Befehl aus.
2. Füllen Sie den Name Parameter mit einem Namen für Ihren benutzerdefinierten Einblick.
3. Füllen Sie den Filters Parameter aus, um anzugeben, welche Ergebnisse in den Einblick aufgenommen werden sollen.
4. Füllen Sie den GroupByAttribute Parameter aus, um anzugeben, welches Attribut verwendet wird, um die Ergebnisse zu gruppieren, die in den Erkenntnissen enthalten sind.
5. Füllen Sie optional den SortCriteria Parameter aus, um die Ergebnisse nach einem bestimmten Feld zu sortieren.

Im folgenden Beispiel wird ein benutzerdefinierter Einblick erstellt, der wichtige Ergebnisse mit dem AwsIamRole Ressourcentyp enthält. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub create-insight --name "Critical role findings" --filters  
'{"ResourceType": [{ "Comparison": "EQUALS", "Value": "AwsIamRole" }],  
"SeverityLabel": [{"Comparison": "EQUALS", "Value": "CRITICAL"}]}' --group-by-  
attribute "ResourceId"
```

PowerShell

Um einen benutzerdefinierten Einblick zu erstellen (PowerShell)

1. Verwenden Sie das New-SHUBInsight Cmdlet.
2. Füllen Sie den Name Parameter mit einem Namen für Ihren benutzerdefinierten Einblick.
3. Füllen Sie den Filter Parameter aus, um anzugeben, welche Ergebnisse in den Einblick aufgenommen werden sollen.
4. Füllen Sie den GroupByAttribute Parameter aus, um anzugeben, welches Attribut verwendet wird, um die Ergebnisse zu gruppieren, die in den Erkenntnissen enthalten sind.

Wenn Sie die [regionsübergreifende Aggregation](#) aktiviert haben und dieses Cmdlet aus der Aggregationsregion verwenden, bezieht sich die Information auf übereinstimmende Ergebnisse aus der Aggregation und verknüpften Regionen.

Beispiel

```
$Filter = @{
    AwsAccountId = [Amazon.SecurityHub.Model.StringFilter]{
        Comparison = "EQUALS"
        Value = "XXX"
    }
    ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]{
        Comparison = "EQUALS"
        Value = 'FAILED'
    }
}
New-SHUBInsight -Filter $Filter -Name TestInsight -GroupByAttribute ResourceId
```

Erstellen eines benutzerdefinierten Insights aus einem verwalteten Insight (nur Konsole)

Sie können keine Änderungen an einem verwalteten Insight speichern oder löschen. Sie können jedoch einen verwalteten Einblick als Grundlage für einen benutzerdefinierten Einblick verwenden. Diese Option ist nur auf der Security Hub CSPM-Konsole verfügbar.

Um einen benutzerdefinierten Insight aus einem verwalteten Insight (Konsole) zu erstellen

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Insights aus.
3. Wählen Sie die verwalteten Insights aus, von denen aus Sie arbeiten möchten.
4. Bearbeiten Sie die Insight-Konfiguration nach Bedarf.
 - So ändern Sie das Attribut, das zum Gruppieren von Ergebnissen in dem Insight verwendet wird:
 - a. Um die bestehende Gruppierung zu entfernen, wählen Sie das X neben der Einstellung Gruppieren aus.
 - b. Wählen Sie das Suchfeld.

- c. Wählen Sie das Attribut aus, das für die Gruppierung verwendet werden soll.
 - d. Wählen Sie Anwenden aus.
- Um einen Filter aus dem Insight zu entfernen, wählen Sie das eingekreiste X neben dem Filter aus.
- So fügen Sie dem Insight einen Filter hinzu:
 - a. Wählen Sie das Suchfeld.
 - b. Wählen Sie das Attribut und den Wert aus, die als Filter verwendet werden sollen.
 - c. Wählen Sie Anwenden aus.
- 5. Wenn Ihre Aktualisierungen abgeschlossen sind, wählen Sie Create insight (Insight erstellen).
- 6. Wenn Sie dazu aufgefordert werden, geben Sie einen Insight-Namen ein und wählen Sie dann Insight erstellen aus.

Einen benutzerdefinierten Einblick bearbeiten

Sie können einen vorhandenen benutzerdefinierten Einblick bearbeiten, um den Gruppierungswert und die Filter zu ändern. Nachdem Sie die Änderungen vorgenommen haben, können Sie die Aktualisierungen an den ursprünglichen Insight speichern oder die aktualisierte Version als neuen Insight speichern.

In AWS Security Hub Cloud Security Posture Management (CSPM) können benutzerdefinierte Erkenntnisse verwendet werden, um bestimmte Ergebnisse zu sammeln und Probleme zu verfolgen, die nur in Ihrer Umgebung auftreten. Hintergrundinformationen zu benutzerdefinierten Erkenntnissen finden Sie unter: [Grundlegendes zu benutzerdefinierten Erkenntnissen in Security Hub CSPM](#)

Um einen benutzerdefinierten Einblick zu bearbeiten, wählen Sie Ihre bevorzugte Methode und folgen Sie den Anweisungen.

Security Hub CSPM console

Um einen benutzerdefinierten Einblick zu bearbeiten (Konsole)

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter: <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Insights aus.
3. Wählen Sie den zu ändernden benutzerdefinierten Insight aus.
4. Bearbeiten Sie die Insight-Konfiguration nach Bedarf.

- So ändern Sie das Attribut, das zum Gruppieren von Ergebnissen in dem Insight verwendet wird:
 - a. Um die bestehende Gruppierung zu entfernen, wählen Sie das X neben der Einstellung Gruppieren aus.
 - b. Wählen Sie das Suchfeld.
 - c. Wählen Sie das Attribut aus, das für die Gruppierung verwendet werden soll.
 - d. Wählen Sie Anwenden aus.
 - Um einen Filter aus dem Insight zu entfernen, wählen Sie das eingekreiste X neben dem Filter aus.
 - So fügen Sie dem Insight einen Filter hinzu:
 - a. Wählen Sie das Suchfeld.
 - b. Wählen Sie das Attribut und den Wert aus, die als Filter verwendet werden sollen.
 - c. Wählen Sie Anwenden aus.
5. Wenn Sie die Aktualisierungen abgeschlossen haben, wählen Sie Save insight (Insight speichern).
 6. Führen Sie eine der folgenden Aktionen aus, wenn Sie dazu aufgefordert werden:
 - Um den vorhandenen Einblick an Ihre Änderungen anzupassen, wählen Sie Aktualisieren **<Insight_Name>** und dann Einblick speichern.
 - Um einen neuen Insight mit den Updates zu erstellen, wählen Sie Save new insight (Neuen Insight speichern). Geben Sie einen Insight name (Insight-Namen) an und wählen Sie dann Save insight (Insight speichern) aus.

Security Hub CSPM API

Um einen benutzerdefinierten Einblick (API) zu bearbeiten

1. Verwenden Sie den [UpdateInsight](#) Betrieb der Security Hub CSPM-API. Wenn Sie den Befehl verwenden, führen Sie den AWS CLI [update-insight](#) Befehl aus.
2. Um den benutzerdefinierten Insight zu identifizieren, den Sie aktualisieren möchten, geben Sie den Amazon-Ressourcennamen (ARN) des Insights an. Verwenden Sie die [GetInsights](#) Operation oder den [get-insights](#) Befehl, um den ARN eines benutzerdefinierten Einblicks abzurufen.
3. Aktualisieren Sie die GroupByAttribute Parameter NameFilters, und nach Bedarf.

Im folgenden Beispiel wird der angegebene Insight aktualisiert. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub update-insight --insight-arn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" --filters '{"ResourceType": [{ "Comparison": "EQUALS", "Value": "AwsIamRole"}], "SeverityLabel": [{"Comparison": "EQUALS", "Value": "HIGH"}]}' --name "High severity role findings"
```

PowerShell

Um einen benutzerdefinierten Einblick zu bearbeiten (PowerShell)

1. Verwenden Sie das Update-SHUBInsight Cmdlet.
2. Um den benutzerdefinierten Insight zu identifizieren, geben Sie den Amazon-Ressourcennamen (ARN) des Insights an. Verwenden Sie das Get-SHUBInsight Cmdlet, um den ARN eines benutzerdefinierten Insights abzurufen.
3. Aktualisieren Sie die GroupByAttribute Parameter NameFilter, und nach Bedarf.

Beispiel

```
$Filter = @{
    ResourceType = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "AwsIamRole"
    }
    SeverityLabel = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "HIGH"
    }
}

Update-SHUBInsight -InsightArn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" -Filter $Filter -Name "High severity role findings"
```

Löschen eines benutzerdefinierten Insights

In AWS Security Hub Cloud Security Posture Management (CSPM) können benutzerdefinierte Erkenntnisse verwendet werden, um bestimmte Ergebnisse zu sammeln und Probleme zu verfolgen, die nur in Ihrer Umgebung auftreten. Hintergrundinformationen zu benutzerdefinierten Erkenntnissen finden Sie unter: [Grundlegendes zu benutzerdefinierten Erkenntnissen in Security Hub CSPM](#)

Um einen benutzerdefinierten Einblick zu löschen, wählen Sie Ihre bevorzugte Methode und folgen Sie den Anweisungen. Sie können einen verwalteten Einblick nicht löschen.

Security Hub CSPM console

Um einen benutzerdefinierten Einblick zu löschen (Konsole)

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter: <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Insights aus.
3. Suchen Sie den benutzerdefinierten Insight, der gelöscht werden soll.
4. Um diesen Einblick zu erhalten, wählen Sie das Symbol für weitere Optionen (die drei Punkte in der oberen rechten Ecke der Karte).
5. Wählen Sie Löschen aus.

Security Hub CSPM API

Um einen benutzerdefinierten Einblick (API) zu löschen

1. Verwenden Sie den [DeleteInsight](#) Betrieb der Security Hub CSPM-API. Wenn Sie den Befehl verwenden, führen Sie den AWS CLI [delete-insight](#) Befehl aus.
2. Geben Sie den ARN des Insights an, um den benutzerdefinierten Insight zu identifizieren, der gelöscht werden soll. Verwenden Sie die [GetInsights](#) Operation oder den [get-insights](#) Befehl, um den ARN eines benutzerdefinierten Einblicks abzurufen.

Im folgenden Beispiel wird der angegebene Insight gelöscht. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub delete-insight --insight-arn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

PowerShell

Um einen benutzerdefinierten Einblick zu löschen () PowerShell

1. Verwenden Sie das Remove-SHUBInsight Cmdlet.
2. Um den benutzerdefinierten Insight zu identifizieren, geben Sie den ARN des Insights an. Verwenden Sie das Get-SHUBInsight Cmdlet, um den ARN eines benutzerdefinierten Insights abzurufen.

Beispiel

```
-InsightArn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Ergebnisse in Security Hub CSPM automatisch ändern und darauf reagieren

AWS Security Hub Cloud Security Posture Management (CSPM) verfügt über Funktionen, die Ergebnisse auf der Grundlage Ihrer Spezifikationen automatisch ändern und entsprechende Maßnahmen ergreifen.

Security Hub CSPM unterstützt derzeit zwei Arten von Automatisierungen:

- **Automatisierungsregeln** — Automatische Aktualisierung und Unterdrückung von Ergebnissen nahezu in Echtzeit auf der Grundlage von von Ihnen definierter Kriterien.
- **Automatisierte Reaktion und Problembehebung** — Erstellen Sie benutzerdefinierte EventBridge Amazon-Regeln, die automatische Maßnahmen definieren, die auf der Grundlage bestimmter Ergebnisse und Erkenntnisse ergriffen werden sollen.

Automatisierungsregeln sind hilfreich, wenn Sie Suchfelder im AWS Security Finding Format (ASFF) automatisch aktualisieren möchten. Sie können beispielsweise eine Automatisierungsregel verwenden, um den Schweregrad oder den Workflow-Status von Ergebnissen aus bestimmten Drittanbieter-Integrationen zu aktualisieren. Durch die Verwendung der Automatisierungsregel entfällt die Notwendigkeit, den Schweregrad oder den Workflow-Status jedes Ergebnisses aus diesem Drittanbieterprodukt manuell zu aktualisieren.

EventBridge Regeln sind hilfreich, wenn Sie außerhalb von Security Hub CSPM Maßnahmen in Bezug auf bestimmte Ergebnisse ergreifen oder bestimmte Ergebnisse zur Behebung oder weiteren Untersuchung an Tools von Drittanbietern senden möchten. Die Regeln können verwendet werden, um unterstützte Aktionen auszulösen, z. B. das Aufrufen einer AWS Lambda Funktion oder die Benachrichtigung eines Amazon Simple Notification Service (Amazon SNS) -Themas über ein bestimmtes Ergebnis.

Automatisierungsregeln werden wirksam, bevor EventBridge Regeln angewendet werden. Das heißt, Automatisierungsregeln werden ausgelöst und aktualisieren ein Ergebnis, bevor das Ergebnis EventBridge empfangen wird. EventBridge Die Regeln gelten dann für den aktualisierten Befund.

Bei der Einrichtung von Automatisierungen für Sicherheitskontrollen empfehlen wir, nach der Kontroll-ID und nicht nach Titel oder Beschreibung zu filtern. Während Security Hub CSPM gelegentlich Kontrolltitel und Beschreibungen aktualisiert, IDs bleibt die Steuerung dieselbe.

Themen

- [Grundlegendes zu den Automatisierungsregeln in Security Hub CSPM](#)
- [Verwendung EventBridge für automatisierte Reaktionen und Problembehebungen](#)

Grundlegendes zu den Automatisierungsregeln in Security Hub CSPM

Sie können Automatisierungsregeln verwenden, um Ergebnisse in AWS Security Hub Cloud Security Posture Management (CSPM) automatisch zu aktualisieren. Bei der Erfassung der Ergebnisse kann Security Hub CSPM eine Vielzahl von Regelaktionen anwenden, z. B. das Unterdrücken von Ergebnissen, das Ändern ihres Schweregrads und das Hinzufügen von Notizen. Solche Regelaktionen ändern Ergebnisse, die Ihren angegebenen Kriterien entsprechen.

Zu den Anwendungsfällen für Automatisierungsregeln gehören unter anderem die folgenden:

- Erhöhung des Schweregrads eines Ergebnisses auf den Wert, CRITICAL wenn sich die Ressourcen-ID des Ergebnisses auf eine geschäftskritische Ressource bezieht.
- Erhöhung des Schweregrads eines Ergebnisses von bis HIGH zu, CRITICAL wenn das Ergebnis Ressourcen in bestimmten Produktionskonten betrifft.
- Zuweisen bestimmter Ergebnisse, deren Schweregrad einem INFORMATIONAL SUPPRESSED Workflow-Status entspricht.

Sie können Automatisierungsregeln nur über ein Security Hub CSPM-Administratorkonto erstellen und verwalten.

Die Regeln gelten sowohl für neue als auch für aktualisierte Ergebnisse. Sie können eine benutzerdefinierte Regel von Grund auf neu erstellen oder eine von Security Hub CSPM bereitgestellte Regelvorlage verwenden. Sie können auch mit einer Vorlage beginnen und diese nach Bedarf ändern.

Definition von Regelkriterien und Regelaktionen

Von einem Security Hub CSPM-Administratorkonto aus können Sie eine Automatisierungsregel erstellen, indem Sie ein oder mehrere Regelkriterien und eine oder mehrere Regelaktionen definieren. Wenn ein Ergebnis den definierten Kriterien entspricht, wendet Security Hub CSPM die

Regelaktionen darauf an. Weitere Informationen zu verfügbaren Kriterien und Aktionen finden Sie unter. [Verfügbare Regelkriterien und Regelaktionen](#)

Security Hub CSPM unterstützt derzeit maximal 100 Automatisierungsregeln für jedes Administratorkonto.

Das Security Hub CSPM-Administratorkonto kann auch Automatisierungsregeln bearbeiten, anzeigen und löschen. Eine Regel gilt für den Abgleich von Ergebnissen im Administratorkonto und all seinen Mitgliedskonten. Durch die Angabe des Mitgliedskontos IDs als Regelkriterium können Security Hub CSPM-Administratoren auch Automatisierungsregeln verwenden, um Ergebnisse in bestimmten Mitgliedskonten zu aktualisieren oder zu unterdrücken.

Eine Automatisierungsregel gilt nur in dem Land, AWS-Region in dem sie erstellt wurde. Um eine Regel in mehreren Regionen anzuwenden, muss der Administrator die Regel in jeder Region erstellen. Dies kann über die Security Hub CSPM-Konsole, die Security Hub CSPM-API oder erfolgen. [AWS CloudFormation Sie können auch ein Bereitstellungsskript für mehrere Regionen verwenden.](#)

Verfügbare Regelkriterien und Regelaktionen

Die folgenden ASFF-Felder (AWS Security Finding Format) werden derzeit als Kriterien für Automatisierungsregeln unterstützt:

Regelkriterium	Operatoren filtern	Feldtyp
AwsAccountId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
AwsAccountName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
CompanyName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge

Regelkriterium	Operatoren filtern	Feldtyp
ComplianceAssociatedStandardsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
ComplianceSecurityControlId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ComplianceStatus	Is, Is Not	Wählen Sie: [FAILED,NOT_AVAILABLE ,PASSED,WARNING]
Confidence	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Anzahl
CreatedAt	Start, End, DateRange	Datum (formatiert als 2021-12-01T 21:47:39.269 Z)
Criticality	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Anzahl
Description	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
FirstObservedAt	Start, End, DateRange	Datum (formatiert als 2021-12-01T 21:47:39.269 Z)

Regelkriterium	Operatoren filtern	Feldtyp
GeneratorId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
Id	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
LastObservedAt	Start, End, DateRange	Datum (formatiert als 2021-12-01T 21:47:39.269 Z)
NoteText	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
NoteUpdatedAt	Start, End, DateRange	Datum (formatiert als 2021-12-01T 21:47:39.269 Z)
NoteUpdatedBy	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
ProductName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge

Regelkriterium	Operatoren filtern	Feldtyp
RecordState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
RelatedFindingsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
RelatedFindingsProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
ResourceApplicationArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
ResourceApplicationName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceDetailsOther	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Zuordnung
ResourceId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Regelkriterium	Operatoren filtern	Feldtyp
ResourcePartition	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
ResourceRegion	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceTags	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Zuordnung
ResourceType	Is, Is Not	Wählen Sie (siehe Von ASFF unterstützte Ressourcen)
SeverityLabel	Is, Is Not	Wählen Sie: [CRITICAL,HIGH,, MEDIUMLOW,INFORMATIONAL]
SourceUrl	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
Title	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
Type	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Regelkriterium	Operatoren filtern	Feldtyp
UpdatedAt	Start, End, DateRange	Datum (formatiert als 2021-12-01T 21:47:39.269 Z)
UserDefinedFields	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Zuordnung
VerificationState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
WorkflowStatus	Is, Is Not	Wählen Sie NEW NOTIFIEDRESOLVED: [,,SUPPRESSED]

Bei Kriterien, die als Zeichenkettenfelder gekennzeichnet sind, wirkt sich die Verwendung verschiedener Filteroperatoren für dasselbe Feld auf die Bewertungslogik aus. Weitere Informationen finden Sie [StringFilter](#) in der AWS Security Hub Cloud Security Posture Management (CSPM) API-Referenz.

Jedes Kriterium unterstützt eine maximale Anzahl von Werten, anhand derer übereinstimmende Ergebnisse gefiltert werden können. Die Grenzwerte für die einzelnen Kriterien finden Sie [AutomationRulesFindingFilters](#) in der AWS Security Hub Cloud Security Posture Management (CSPM) API-Referenz.

Die folgenden ASFF-Felder werden derzeit als Aktionen für Automatisierungsregeln unterstützt:

- Confidence
- Criticality
- Note
- RelatedFindings
- Severity
- Types
- UserDefinedFields

- `VerificationState`
- `Workflow`

Weitere Informationen zu bestimmten ASFF-Feldern finden Sie unter Syntax des [AWS Security Finding Format \(ASFF\)](#).

 Tip

Wenn Sie möchten, dass Security Hub CSPM keine Ergebnisse für ein bestimmtes Steuerelement generiert, empfehlen wir, das Steuerelement zu deaktivieren, anstatt eine Automatisierungsregel zu verwenden. Wenn Sie eine Kontrolle deaktivieren, beendet Security Hub CSPM die Durchführung von Sicherheitsüberprüfungen und generiert keine Ergebnisse mehr dafür, sodass Ihnen für diese Kontrolle keine Gebühren entstehen. Wir empfehlen die Verwendung von Automatisierungsregeln, um die Werte bestimmter ASFF-Felder für Ergebnisse zu ändern, die definierten Kriterien entsprechen. Weitere Informationen zum Deaktivieren von Steuerelementen finden Sie unter [Steuerelemente in Security Hub CSPM deaktivieren](#).

Ergebnisse, die durch Automatisierungsregeln bewertet werden

Eine Automatisierungsregel wertet neue und aktualisierte Ergebnisse aus, die Security Hub CSPM im Rahmen des [BatchImportFindings](#) Vorgangs generiert oder aufnimmt, nachdem Sie die Regel erstellt haben. Security Hub CSPM-Updates kontrollieren die Ergebnisse alle 12 bis 24 Stunden oder wenn sich der Status der zugehörigen Ressource ändert. Weitere Informationen finden Sie unter [Zeitplan für die Ausführung von Sicherheitsprüfungen](#).

Automatisierungsregeln bewerten die ursprünglichen Ergebnisse, die vom Anbieter bereitgestellt wurden. Durch den `BatchImportFindings` Betrieb der Security Hub CSPM-API können Anbieter neue Erkenntnisse bereitstellen und bestehende Erkenntnisse aktualisieren. Regeln werden nicht ausgelöst, wenn Sie Suchfelder nach der Regelerstellung im Rahmen des [BatchUpdateFindings](#) Vorgangs aktualisieren. Wenn Sie eine Automatisierungsregel erstellen und eine `BatchUpdateFindings` Aktualisierung vornehmen, die sich beide auf dasselbe Ergebnisfeld auswirken, legt die letzte Aktualisierung den Wert für dieses Feld fest. Nehmen wir das folgende Beispiel:

1. Sie verwenden `BatchUpdateFindings`, um das `Workflow.Status` Feld eines Befundes von `NEW` zu `NOTIFIED` zu aktualisieren.
2. Wenn Sie aufrufen `GetFindings`, hat das `Workflow.Status` Feld jetzt den Wert `NOTIFIED`.
3. Sie erstellen eine Automatisierungsregel, die das `Workflow.Status` Feld des Ergebnisses von `NEW` zu `SUPPRESSED` ändert (denken Sie daran, dass Regeln Aktualisierungen ignorieren, die mit `BatchUpdateFindings` vorgenommen wurden).
4. Der Suchdienstleister verwendet `BatchImportFindings`, um den Befund zu aktualisieren, und ändert das `Workflow.Status` Feld in `NEW`.
5. Wenn Sie aufrufen `GetFindings`, hat das `Workflow.Status` Feld jetzt den Wert `SUPPRESSED` weil die Automatisierungsregel angewendet wurde und die Regel die letzte Aktion war, die für das Ergebnis ausgeführt wurde.

Wenn Sie eine Regel auf der Security Hub CSPM-Konsole erstellen oder bearbeiten, zeigt die Konsole eine Betaversion von Ergebnissen an, die den Regelkriterien entsprechen. Während Automatisierungsregeln die ursprünglichen Ergebnisse auswerten, die vom Finding-Anbieter gesendet wurden, spiegelt die Betaversion der Konsole die Ergebnisse in ihrem endgültigen Zustand wider, so wie sie als Antwort auf den [GetFindings](#) API-Vorgang angezeigt würden (d. h. nachdem Regelaktionen oder andere Updates auf das Ergebnis angewendet wurden).

Wie funktioniert die Reihenfolge der Regeln

Beim Erstellen von Automatisierungsregeln weisen Sie jeder Regel eine Reihenfolge zu. Dies bestimmt die Reihenfolge, in der Security Hub CSPM Ihre Automatisierungsregeln anwendet, und ist wichtig, wenn sich mehrere Regeln auf dasselbe Such- oder Findungsfeld beziehen.

Wenn sich mehrere Regelaktionen auf dasselbe Befund- oder Findungsfeld beziehen, gilt die Regel mit dem höchsten numerischen Wert für die Reihenfolge der Regeln zuletzt und hat die endgültige Wirkung.

Wenn Sie eine Regel in der Security Hub CSPM-Konsole erstellen, weist Security Hub CSPM automatisch die Regelreihenfolge auf der Grundlage der Reihenfolge der Regelerstellung zu. Die zuletzt erstellte Regel hat den niedrigsten numerischen Wert für die Regelreihenfolge und gilt daher zuerst. Security Hub CSPM wendet nachfolgende Regeln in aufsteigender Reihenfolge an.

Wenn Sie eine Regel über die Security Hub CSPM API oder erstellen AWS CLI, wendet Security Hub CSPM zuerst die Regel mit dem niedrigsten numerischen Wert an. Anschließend werden die nachfolgenden Regeln in aufsteigender Reihenfolge angewendet. Wenn mehrere

Ergebnisse identisch sind `RuleOrder`, wendet Security Hub CSPM zuerst eine Regel mit einem früheren Wert für das `UpdatedAt` Feld an (d. h. die Regel, die zuletzt bearbeitet wurde, gilt zuletzt).

Sie können die Reihenfolge der Regeln jederzeit ändern.

Beispiel für die Reihenfolge der Regeln:

Regel A (Reihenfolge ist **1**):

- Kriterien für Regel A
 - `ProductName = Security Hub CSPM`
 - `Resources.Type` ist `S3 Bucket`
 - `Compliance.Status = FAILED`
 - `RecordState` ist `NEW`
 - `Workflow.Status = ACTIVE`
- Aktionen nach Regel A
 - Update Confidence auf 95
 - Aktualisieren Severity auf `CRITICAL`

Regel B (Reihenfolge der Regeln ist **2**):

- Kriterien für Regel B
 - `AwsAccountId = 123456789012`
- Aktionen nach Regel B
 - Update Severity auf `INFORMATIONAL`

Aktionen nach Regel A gelten zuerst für Security Hub CSPM-Ergebnisse, die den Kriterien von Regel A entsprechen. Als Nächstes gelten die Aktionen nach Regel B für Security Hub CSPM-Ergebnisse mit der angegebenen Konto-ID. Da Regel B in diesem Beispiel zuletzt gilt, lautet der Endwert für Ergebnisse aus Severity der angegebenen Konto-ID. `INFORMATIONAL` Basierend auf der Regel A-Aktion ist der Endwert von Confidence in übereinstimmenden Ergebnissen 95.

Automatisierungsregeln erstellen

Eine Automatisierungsregel kann verwendet werden, um Ergebnisse in AWS Security Hub Cloud Security Posture Management (CSPM) automatisch zu aktualisieren. Sie können eine

benutzerdefinierte Automatisierungsregel von Grund auf neu erstellen oder in der Security Hub CSPM-Konsole eine vorab ausgefüllte Regelvorlage verwenden. Hintergrundinformationen zur Funktionsweise von Automatisierungsregeln finden Sie unter. [Grundlegendes zu den Automatisierungsregeln in Security Hub CSPM](#)

Sie können jeweils nur eine Automatisierungsregel erstellen. Um mehrere Automatisierungsregeln zu erstellen, folgen Sie den Konsolenprozeduren mehrmals oder rufen Sie die API oder den Befehl mehrmals mit den gewünschten Parametern auf.

Sie müssen in jeder Region und jedem Konto, in dem die Regel auf Ergebnisse angewendet werden soll, eine Automatisierungsregel erstellen.

Wenn Sie eine Automatisierungsregel in der Security Hub CSPM-Konsole erstellen, zeigt Ihnen Security Hub CSPM eine Betaversion der Ergebnisse, für die Ihre Regel gilt. Die Betaversion wird derzeit nicht unterstützt, wenn Ihre Regelkriterien einen CONTAINS- oder NOT_CONTAINS-Filter beinhalten. Sie können diese Filter für Zuordnungs- und Zeichenkettenfeldtypen auswählen.

 Important

AWS empfiehlt, keine personenbezogenen, vertraulichen oder sensiblen Informationen in den Regelnamen, die Beschreibung oder andere Felder aufzunehmen.

Eine benutzerdefinierte Automatisierungsregel erstellen

Wählen Sie Ihre bevorzugte Methode und führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Automatisierungsregel zu erstellen.

Console

So erstellen Sie eine benutzerdefinierte Automatisierungsregel (Konsole)

1. Öffnen Sie mit den Anmeldeinformationen des Security Hub CSPM-Administrators die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Automations aus.
3. Wählen Sie Regel erstellen aus. Wählen Sie für Regeltyp die Option Benutzerdefinierte Regel erstellen aus.

4. Geben Sie im Abschnitt Regel einen eindeutigen Regelnamen und eine Beschreibung für Ihre Regel ein.
5. Verwenden Sie für Kriterien die Dropdownmenüs Schlüssel, Operator und Wert, um Ihre Regelkriterien anzugeben. Sie müssen mindestens ein Regelkriterium angeben.

Wenn die von Ihnen ausgewählten Kriterien unterstützt werden, zeigt Ihnen die Konsole eine Betaversion der Ergebnisse, die Ihren Kriterien entsprechen.

6. Verwenden Sie für automatisierte Aktionen die Dropdownmenüs, um anzugeben, welche Ergebnisfelder aktualisiert werden sollen, wenn die Ergebnisse Ihren Regelkriterien entsprechen. Sie müssen mindestens eine Regelaktion angeben.
7. Wählen Sie unter Regelstatus aus, ob die Regel nach ihrer Erstellung aktiviert oder deaktiviert werden soll.
8. (Optional) Erweitern Sie den Abschnitt Zusätzliche Einstellungen. Wählen Sie Nachfolgende Regeln für Ergebnisse ignorieren, die diesen Kriterien entsprechen, wenn diese Regel die letzte Regel sein soll, die auf Ergebnisse angewendet wird, die den Regelkriterien entsprechen.
9. (Optional) Fügen Sie für Tags Tags als Schlüssel-Wert-Paare hinzu, damit Sie die Regel leichter identifizieren können.
10. Wählen Sie Regel erstellen aus.

API

Um eine benutzerdefinierte Automatisierungsregel (API) zu erstellen

1. Führen Sie die Ausführung [CreateAutomationRule](#) über das Security Hub CSPM-Administratorkonto aus. Diese API erstellt eine Regel mit einem bestimmten Amazon-Ressourcennamen (ARN).
2. Geben Sie einen Namen und eine Beschreibung für die Regel ein.
3. Legen Sie den `IsTerminal` Parameter auf fest, `true` wenn diese Regel die letzte Regel sein soll, die auf Ergebnisse angewendet wird, die den Regelkriterien entsprechen.
4. Geben Sie für den `RuleOrder` Parameter die Reihenfolge der Regel an. Security Hub CSPM wendet zuerst Regeln mit einem niedrigeren numerischen Wert für diesen Parameter an.
5. Geben Sie für den `RuleStatus` Parameter an, ob Security Hub CSPM die Regel aktivieren und nach der Erstellung auf Ergebnisse anwenden soll. Der Standardwert ist `ENABLED`, wenn

kein Wert angegeben wird. Der Wert von DISABLED bedeutet, dass die Regel nach der Erstellung angehalten wird.

6. Geben Sie für den Criteria Parameter die Kriterien an, nach denen Security Hub CSPM Ihre Ergebnisse filtern soll. Die Regelaktion gilt für Ergebnisse, die den Kriterien entsprechen. Eine Liste der unterstützten Kriterien finden Sie unter [Verfügbare Regelkriterien und Regelaktionen](#).
7. Geben Sie für den Actions Parameter die Aktionen an, die Security Hub CSPM ausführen soll, wenn eine Übereinstimmung zwischen einem Ergebnis und Ihren definierten Kriterien besteht. Eine Liste der unterstützten Aktionen finden Sie unter [Verfügbare Regelkriterien und Regelaktionen](#).

Mit dem folgenden AWS CLI Beispielbefehl wird eine Automatisierungsregel erstellt, die den Workflow-Status und die Notiz der übereinstimmenden Ergebnisse aktualisiert. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub create-automation-rule \
--actions '[{
  "Type": "FINDING_FIELDS_UPDATE",
  "FindingFieldsUpdate": {
    "Severity": {
      "Label": "HIGH"
    },
    "Note": {
      "Text": "Known issue that is a risk. Updated by automation rules",
      "UpdatedBy": "sechub-automation"
    }
  }
}]' \
--criteria '{
  "SeverityLabel": [{
    "Value": "INFORMATIONAL",
    "Comparison": "EQUALS"
  }]
}' \
--description "A sample rule" \
--no-is-terminal \
--rule-name "sample rule" \
--rule-order 1 \
--rule-status "ENABLED" \
```

```
--region us-east-1
```

Eine Automatisierungsregel anhand einer Vorlage erstellen (nur Konsole)

Regelvorlagen spiegeln gängige Anwendungsfälle für Automatisierungsregeln wider. Derzeit unterstützt nur die Security Hub CSPM-Konsole Regelvorlagen. Gehen Sie wie folgt vor, um eine Automatisierungsregel aus einer Vorlage in der Konsole zu erstellen.

Um eine Automatisierungsregel aus einer Vorlage (Konsole) zu erstellen

1. Öffnen Sie mit den Anmeldeinformationen des Security Hub CSPM-Administrators die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Automations aus.
3. Wählen Sie Regel erstellen aus. Wählen Sie als Regeltyp die Option Regel aus Vorlage erstellen aus.
4. Wählen Sie im Dropdownmenü eine Regelvorlage aus.
5. (Optional) Falls für Ihren Anwendungsfall erforderlich, ändern Sie die Abschnitte Regel, Kriterien und Automatisierte Aktion. Sie müssen mindestens ein Regelkriterium und eine Regelaktion angeben.

Wenn die von Ihnen ausgewählten Kriterien unterstützt werden, zeigt Ihnen die Konsole eine Betaversion der Ergebnisse, die Ihren Kriterien entsprechen.

6. Wählen Sie unter Regelstatus aus, ob die Regel nach ihrer Erstellung aktiviert oder deaktiviert werden soll.
7. (Optional) Erweitern Sie den Abschnitt Zusätzliche Einstellungen. Wählen Sie Nachfolgende Regeln für Ergebnisse ignorieren, die diesen Kriterien entsprechen, wenn diese Regel die letzte Regel sein soll, die auf Ergebnisse angewendet wird, die den Regelkriterien entsprechen.
8. (Optional) Fügen Sie für Tags Tags als Schlüssel-Wert-Paare hinzu, damit Sie die Regel leichter identifizieren können.
9. Wählen Sie Regel erstellen aus.

Automatisierungsregeln anzeigen

Eine Automatisierungsregel kann verwendet werden, um Ergebnisse in AWS Security Hub Cloud Security Posture Management (CSPM) automatisch zu aktualisieren. Hintergrundinformationen zur Funktionsweise von Automatisierungsregeln finden Sie unter [Grundlegendes zu den Automatisierungsregeln in Security Hub CSPM](#)

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um Ihre vorhandenen Automatisierungsregeln und die Details jeder Regel einzusehen.

Einen Überblick darüber, wie Automatisierungsregeln Ihre Ergebnisse verändert haben, finden Sie unter [Überprüfung der Funddetails und des Verlaufs in Security Hub CSPM](#).

Console

So zeigen Sie Automatisierungsregeln an (Konsole)

1. Öffnen Sie mit den Anmeldeinformationen des Security Hub CSPM-Administrators die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Automations aus.
3. Wählen Sie einen Regelnamen. Wählen Sie alternativ eine Regel aus.
4. Wählen Sie Aktionen und Ansicht aus.

API

Um Automatisierungsregeln (API) anzuzeigen

1. Um die Automatisierungsregeln für Ihr Konto einzusehen, führen Sie es [ListAutomationRules](#) vom Security Hub CSPM-Administratorkonto aus. Diese API gibt die Regel ARNs und andere Metadaten für Ihre Regeln zurück. Für diese API sind keine Eingabeparameter erforderlich, Sie können diese jedoch optional NextToken als Paginierungsparameter angeben, MaxResults um die Anzahl der Ergebnisse zu begrenzen. Der Anfangswert von NextToken sollte sein. NULL
2. Weitere Regeldetails, einschließlich der Kriterien und Aktionen für eine Regel, erhalten Sie [BatchGetAutomationRules](#) über das Security Hub CSPM-Administratorkonto. Geben Sie ARNs die Automatisierungsregeln an, für die Sie Details benötigen.

Im folgenden Beispiel werden Details für die angegebenen Automatisierungsregeln abgerufen. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub batch-get-automation-rules \
--automation-rules-arns '["arn:aws:securityhub:us-
east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
"arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-
cdef-EXAMPLE22222"]' \
--region us-east-1
```

Automatisierungsregeln bearbeiten

Eine Automatisierungsregel kann verwendet werden, um Ergebnisse in AWS Security Hub Cloud Security Posture Management (CSPM) automatisch zu aktualisieren. Hintergrundinformationen zur Funktionsweise von Automatisierungsregeln finden Sie unter [Grundlegendes zu den Automatisierungsregeln in Security Hub CSPM](#)

Nach der Erstellung einer Automatisierungsregel kann der delegierte Security Hub CSPM-Administrator die Regel bearbeiten. Wenn Sie eine Automatisierungsregel bearbeiten, gelten die Änderungen für neue und aktualisierte Ergebnisse, die Security Hub CSPM nach der Regelbearbeitung generiert oder aufnimmt.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um den Inhalt einer Automatisierungsregel zu bearbeiten. Sie können eine oder mehrere Regeln mit einer einzigen Anfrage bearbeiten. Anweisungen zum Bearbeiten der Reihenfolge finden Sie unter [Reihenfolge der Automatisierungsregeln bearbeiten](#).

Console

So bearbeiten Sie Automatisierungsregeln (Konsole)

1. Öffnen Sie mit den Anmeldeinformationen des Security Hub CSPM-Administrators die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Automations aus.
3. Wählen Sie die Regel aus, die Sie bearbeiten möchten. Wählen Sie Aktion und Bearbeiten.

4. Ändern Sie die Regel wie gewünscht und wählen Sie Änderungen speichern.

API

Um Automatisierungsregeln (API) zu bearbeiten

1. Führen Sie die Ausführung [BatchUpdateAutomationRules](#) über das Security Hub CSPM-Administratorkonto aus.
2. Geben Sie für den RuleArn Parameter den ARN der Regel (n) an, die Sie bearbeiten möchten.
3. Geben Sie die neuen Werte für die Parameter an, die Sie bearbeiten möchten. Sie können jeden Parameter bearbeiten, außer RuleArn.

Im folgenden Beispiel wird die angegebene Automatisierungsregel aktualisiert. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub batch-update-automation-rules \
--update-automation-rules-request-items '[
  {
    "Actions": [{
      "Type": "FINDING_FIELDS_UPDATE",
      "FindingFieldsUpdate": {
        "Note": {
          "Text": "Known issue that is a risk",
          "UpdatedBy": "sechub-automation"
        },
        "Workflow": {
          "Status": "NEW"
        }
      }
    }],
    "Criteria": {
      "SeverityLabel": [{
        "Value": "LOW",
        "Comparison": "EQUALS"
      }]
    },
    "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
```

```
"RuleOrder": 14,  
"RuleStatus": "DISABLED",  
}  
]' \  
--region us-east-1
```

Reihenfolge der Automatisierungsregeln bearbeiten

Eine Automatisierungsregel kann verwendet werden, um Ergebnisse in AWS Security Hub Cloud Security Posture Management (CSPM) automatisch zu aktualisieren. Hintergrundinformationen zur Funktionsweise von Automatisierungsregeln finden Sie unter. [Grundlegendes zu den Automatisierungsregeln in Security Hub CSPM](#)

Nach der Erstellung einer Automatisierungsregel kann der delegierte Security Hub CSPM-Administrator die Regel bearbeiten.

Wenn Sie die Regelkriterien und Aktionen unverändert lassen möchten, aber die Reihenfolge ändern möchten, in der Security Hub CSPM eine Automatisierungsregel anwendet, können Sie nur die Reihenfolge der Regeln bearbeiten. Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um die Reihenfolge der Regeln zu bearbeiten.

Anweisungen zum Bearbeiten der Kriterien oder Aktionen einer Automatisierungsregel finden Sie unter [Automatisierungsregeln bearbeiten](#).

Console

So bearbeiten Sie die Reihenfolge der Automatisierungsregeln (Konsole)

1. Öffnen Sie mit den Anmeldeinformationen des Security Hub CSPM-Administrators die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Automations aus.
3. Wählen Sie die Regel aus, deren Reihenfolge Sie ändern möchten. Wählen Sie Priorität bearbeiten.
4. Wählen Sie Nach oben, um die Priorität der Regel um eine Einheit zu erhöhen. Wählen Sie Nach unten, um die Priorität der Regel um eine Einheit zu verringern. Wählen Sie „Nach oben“, um der Regel die Reihenfolge 1 zuzuweisen (dadurch hat die Regel Vorrang vor anderen bestehenden Regeln).

 Note

Wenn Sie eine Regel in der Security Hub CSPM-Konsole erstellen, weist Security Hub CSPM automatisch die Regelreihenfolge auf der Grundlage der Reihenfolge der Regelerstellung zu. Die zuletzt erstellte Regel hat den niedrigsten numerischen Wert für die Regelreihenfolge und gilt daher zuerst.

API

Um die Reihenfolge der Automatisierungsregeln (API) zu bearbeiten

1. Verwenden Sie den [BatchUpdateAutomationRules](#) Vorgang vom Security Hub CSPM-Administratorkonto aus.
2. Geben Sie für den `RuleArn` Parameter den ARN der Regel (n) an, deren Reihenfolge Sie bearbeiten möchten.
3. Ändern Sie den Wert des `RuleOrder` Felds.

 Note

Wenn mehrere Regeln dasselbe haben `RuleOrder`, wendet Security Hub CSPM zuerst eine Regel mit einem früheren Wert für das `UpdatedAt` Feld an (d. h. die Regel, die zuletzt bearbeitet wurde, gilt zuletzt).

Automatisierungsregeln löschen oder deaktivieren

Eine Automatisierungsregel kann verwendet werden, um Ergebnisse in AWS Security Hub Cloud Security Posture Management (CSPM) automatisch zu aktualisieren. Hintergrundinformationen zur Funktionsweise von Automatisierungsregeln finden Sie unter. [Grundlegendes zu den Automatisierungsregeln in Security Hub CSPM](#)

Wenn Sie eine Automatisierungsregel löschen, entfernt Security Hub CSPM sie aus Ihrem Konto und wendet die Regel nicht mehr auf Ergebnisse an. Als Alternative zum Löschen können Sie eine Regel deaktivieren. Dadurch wird die Regel für die future Verwendung beibehalten, aber Security Hub CSPM wendet die Regel erst auf übereinstimmende Ergebnisse an, wenn Sie sie aktivieren.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten zum Löschen einer Automatisierungsregel. Sie können eine oder mehrere Regeln in einer einzigen Anfrage löschen.

Console

Um Automatisierungsregeln zu löschen oder zu deaktivieren (Konsole)

1. Öffnen Sie mit den Anmeldeinformationen des Security Hub CSPM-Administrators die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Automations aus.
3. Wählen Sie die Regel (n) aus, die Sie löschen möchten. Wählen Sie Aktion und Löschen (um eine Regel beizubehalten, sie aber vorübergehend zu deaktivieren, wählen Sie Deaktivieren).
4. Bestätigen Sie Ihre Wahl und wählen Sie Delete (Löschen) aus.

API

Um Automatisierungsregeln (API) zu löschen oder zu deaktivieren

1. Verwenden Sie den [BatchDeleteAutomationRules](#) Vorgang vom Security Hub CSPM-Administratorkonto aus.
2. Geben Sie für den AutomationRulesArns Parameter den ARN der Regel (n) an, die Sie löschen möchten (um eine Regel beizubehalten, sie aber vorübergehend zu deaktivieren, geben DISABLED Sie den RuleStatus Parameter an).

Im folgenden Beispiel wird die angegebene Automatisierungsregel gelöscht. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub batch-delete-automation-rules \
--automation-rules-arns '["arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE1111"]' \
--region us-east-1
```

Beispiele für Automatisierungsregeln

Dieser Abschnitt enthält Beispiele für Automatisierungsregeln für gängige Security Hub CSPM-Anwendungsfälle. Diese Beispiele entsprechen Regelvorlagen, die auf der Security Hub CSPM-Konsole verfügbar sind.

Erhöhen Sie den Schweregrad auf Kritisch, wenn eine bestimmte Ressource, z. B. ein S3-Bucket, gefährdet ist

In diesem Beispiel werden die Regelkriterien erfüllt, wenn es sich ResourceId bei einem Ergebnis um einen bestimmten Amazon Simple Storage Service (Amazon S3) -Bucket handelt. Die Regelaktion besteht darin, den Schweregrad der übereinstimmenden Ergebnisse auf zu ändern CRITICAL. Sie können diese Vorlage ändern, um sie auf andere Ressourcen anzuwenden.

Beispiel für eine API-Anfrage:

```
{
  "IsTerminal": true,
  "RuleName": "Elevate severity of findings that relate to important resources",
  "RuleOrder": 1,
  "RuleStatus": "ENABLED",
  "Description": "Elevate finding severity to CRITICAL when specific resource such as an S3 bucket is at risk",
  "Criteria": {
    "ProductName": [{
      "Value": "Security Hub CSPM",
      "Comparison": "EQUALS"
    }],
    "ComplianceStatus": [{
      "Value": "FAILED",
      "Comparison": "EQUALS"
    }],
    "RecordState": [{
      "Value": "ACTIVE",
      "Comparison": "EQUALS"
    }],
    "WorkflowStatus": [{
      "Value": "NEW",
      "Comparison": "EQUALS"
    }],
    "ResourceId": [{
      "Value": "arn:aws:s3:::amzn-s3-demo-bucket/developers/design_info.doc",
```

```

        "Comparison": "EQUALS"
    }
  ],
  "Actions": [{
    "Type": "FINDING_FIELDS_UPDATE",
    "FindingFieldsUpdate": {
      "Severity": {
        "Label": "CRITICAL"
      },
      "Note": {
        "Text": "This is a critical resource. Please review ASAP.",
        "UpdatedBy": "sechub-automation"
      }
    }
  ]
}

```

Beispiel für einen CLI-Befehl:

```

$
aws securityhub create-automation-rule \
--is-terminal \
--rule-name "Elevate severity of findings that relate to important resources" \
--rule-order 1 \
--rule-status "ENABLED" \

--description "Elevate finding severity to CRITICAL when specific resource such as an
S3 bucket is at risk" \
--criteria '{
  "ProductName": [{
    "Value": "Security Hub CSPM",
    "Comparison": "EQUALS"
  }],
  "ComplianceStatus": [{
    "Value": "FAILED",
    "Comparison": "EQUALS"
  }],
  "RecordState": [{
    "Value": "ACTIVE",
    "Comparison": "EQUALS"
  }],
  "WorkflowStatus": [{
    "Value": "NEW",

```

```

"Comparison": "EQUALS"
}],
"ResourceId": [{
  "Value": "arn:aws:s3:::amzn-s3-demo-bucket/developers/design_info.doc",
  "Comparison": "EQUALS"
}]
}' \
--actions '[{
  "Type": "FINDING_FIELDS_UPDATE",
  "FindingFieldsUpdate": {
    "Severity": {
      "Label": "CRITICAL"
    },
    "Note": {
      "Text": "This is a critical resource. Please review ASAP.",
      "UpdatedBy": "sechub-automation"
    }
  }
}]' \
--region us-east-1

```

Erhöhen Sie den Schweregrad von Feststellungen, die sich auf Ressourcen in Produktionskonten beziehen

In diesem Beispiel werden die Regelkriterien erfüllt, wenn in bestimmten Produktionskonten ein HIGH Schweregrad festgestellt wird. Die Regelaktion besteht darin, den Schweregrad der übereinstimmenden Ergebnisse auf zu ändern CRITICAL.

Beispiel für eine API-Anfrage:

```

{
  "IsTerminal": false,
  "RuleName": "Elevate severity for production accounts",
  "RuleOrder": 1,
  "RuleStatus": "ENABLED",
  "Description": "Elevate finding severity from HIGH to CRITICAL for findings that relate to resources in specific production accounts",
  "Criteria": {
    "ProductName": [{
      "Value": "Security Hub CSPM",
      "Comparison": "EQUALS"
    }],
    "ComplianceStatus": [{

```

```

        "Value": "FAILED",
        "Comparison": "EQUALS"
    ]],
    "RecordState": [{
        "Value": "ACTIVE",
        "Comparison": "EQUALS"
    }],
    "WorkflowStatus": [{
        "Value": "NEW",
        "Comparison": "EQUALS"
    }],
    "SeverityLabel": [{
        "Value": "HIGH",
        "Comparison": "EQUALS"
    }],
    "AwsAccountId": [
        {
            "Value": "111122223333",
            "Comparison": "EQUALS"
        },
        {
            "Value": "123456789012",
            "Comparison": "EQUALS"
        }
    ],
},
"Actions": [{
    "Type": "FINDING_FIELDS_UPDATE",
    "FindingFieldsUpdate": {
        "Severity": {
            "Label": "CRITICAL"
        },
        "Note": {
            "Text": "A resource in production accounts is at risk. Please review
ASAP.",
            "UpdatedBy": "sechub-automation"
        }
    }
}]
}

```

Beispiel für einen CLI-Befehl:


```
aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Elevate severity of findings that relate to resources in production accounts" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Elevate finding severity from HIGH to CRITICAL for findings that relate to resources in specific production accounts" \
--criteria '{
  "ProductName": [{
    "Value": "Security Hub CSPM",
    "Comparison": "EQUALS"
  }],
  "ComplianceStatus": [{
    "Value": "FAILED",
    "Comparison": "EQUALS"
  }],
  "RecordState": [{
    "Value": "ACTIVE",
    "Comparison": "EQUALS"
  }],
  "SeverityLabel": [{
    "Value": "HIGH",
    "Comparison": "EQUALS"
  }],
  "AwsAccountId": [
    {
      "Value": "111122223333",
      "Comparison": "EQUALS"
    },
    {
      "Value": "123456789012",
      "Comparison": "EQUALS"
    }
  ]
}' \
--actions '[{
  "Type": "FINDING_FIELDS_UPDATE",
  "FindingFieldsUpdate": {
    "Severity": {
      "Label": "CRITICAL"
    },
    "Note": {
      "Text": "A resource in production accounts is at risk. Please review ASAP.",
      "UpdatedBy": "sechub-automation"
    }
  }
}]'
```

```

}
}
]]' \
--region us-east-1

```

Informative Ergebnisse unterdrücken

In diesem Beispiel werden die Regelkriterien für die Ergebnisse des INFORMATIONAL Schweregrads, die von Amazon an Security Hub CSPM gesendet wurden, abgeglichen. GuardDuty Die Regelaktion besteht darin, den Workflow-Status der übereinstimmenden Ergebnisse auf zu ändern. SUPPRESSED

Beispiel für eine API-Anfrage:

```

{
  "IsTerminal": false,
  "RuleName": "Suppress informational findings",
  "RuleOrder": 1,
  "RuleStatus": "ENABLED",
  "Description": "Suppress GuardDuty findings with INFORMATIONAL severity",
  "Criteria": {
    "ProductName": [{
      "Value": "GuardDuty",
      "Comparison": "EQUALS"
    }],
    "RecordState": [{
      "Value": "ACTIVE",
      "Comparison": "EQUALS"
    }],
    "WorkflowStatus": [{
      "Value": "NEW",
      "Comparison": "EQUALS"
    }],
    "SeverityLabel": [{
      "Value": "INFORMATIONAL",
      "Comparison": "EQUALS"
    }]
  },
  "Actions": [{
    "Type": "FINDING_FIELDS_UPDATE",
    "FindingFieldsUpdate": {
      "Workflow": {
        "Status": "SUPPRESSED"
      }
    }
  ]
}

```

```

        "Note": {
            "Text": "Automatically suppress GuardDuty findings with INFORMATIONAL
severity",
            "UpdatedBy": "sechub-automation"
        }
    }
}
]]
}

```

Beispiel für einen CLI-Befehl:

```

aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Suppress informational findings" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Suppress GuardDuty findings with INFORMATIONAL severity" \
--criteria '{
"ProductName": [{
"Value": "GuardDuty",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"WorkflowStatus": [{
"Value": "NEW",
"Comparison": "EQUALS"
}],
"SeverityLabel": [{
"Value": "INFORMATIONAL",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {

```

```
"Workflow": {  
  "Status": "SUPPRESSED"  
},  
"Note": {  
  "Text": "Automatically suppress GuardDuty findings with INFORMATIONAL severity",  
  "UpdatedBy": "sechub-automation"  
}  
}  
}]' \  
--region us-east-1
```

Verwendung EventBridge für automatisierte Reaktionen und Problembehebungen

Durch die Erstellung von Regeln in Amazon EventBridge können Sie automatisch auf Ergebnisse von AWS Security Hub Cloud Security Posture Management (CSPM) reagieren. Security Hub CSPM sendet Ergebnisse als Ereignisse nahezu EventBridge in Echtzeit an. Sie können einfache Regeln schreiben, um anzugeben, an welchen Ereignissen Sie interessiert sind und welche automatisierten Aktionen ergriffen werden sollen, wenn ein Ereignis einer Regel entspricht. Die folgenden Aktionen können beispielsweise automatisch ausgelöst werden:

- Eine AWS Lambda Funktion aufrufen
- Aufrufen des Amazon EC2 Run-Befehls
- Weiterleiten des Ereignisses an Amazon Kinesis Data Streams
- Aktivierung einer AWS Step Functions Zustandsmaschine
- Benachrichtigen eines Amazon SNS-Themas oder einer Amazon SQS-Warteschlange
- Senden eines Funds an ein Ticketing-, Chat-, SIEM- oder Incident-Response- und Management-Tool eines Drittanbieters

Security Hub CSPM sendet automatisch alle neuen Erkenntnisse und alle Aktualisierungen vorhandener Ergebnisse EventBridge als EventBridge Ereignisse an. Sie können auch benutzerdefinierte Aktionen erstellen, mit denen Sie ausgewählte Ergebnisse und Insight-Ergebnisse an senden können. EventBridge

Anschließend konfigurieren Sie EventBridge Regeln, um auf jeden Ereignistyp zu reagieren.

Weitere Informationen zur Verwendung EventBridge finden Sie im [EventBridge Amazon-Benutzerhandbuch](#).

 Note

Als bewährte Methode sollten Sie sicherstellen, dass für die Zugriffsberechtigungen, die Ihren Benutzern gewährt werden, IAM-Richtlinien AWS Identity and Access Management (Least-Privilege) EventBridge verwendet werden, die nur die erforderlichen Berechtigungen gewähren.

Weitere Informationen finden Sie unter [Identitäts- und Zugriffsverwaltung in Amazon EventBridge](#).

Eine Reihe von Vorlagen für kontenübergreifende automatisierte Reaktionen und Problembehebungen ist auch unter Lösungen verfügbar. AWS Die Vorlagen nutzen EventBridge Ereignisregeln und Lambda-Funktionen. Sie stellen die Lösung mit AWS CloudFormation und AWS Systems Manager bereit. Die Lösung kann vollautomatische Reaktions- und Abhilfemaßnahmen erstellen. Es kann auch benutzerdefinierte Security Hub CSPM-Aktionen verwenden, um vom Benutzer ausgelöste Reaktions- und Abhilfemaßnahmen zu erstellen. Einzelheiten zur Konfiguration und Verwendung der Lösung finden Sie auf der Lösungsseite [Automated Security Response](#). AWS

Themen

- [Security Hub CSPM-Ereignistypen in EventBridge](#)
- [EventBridge Veranstaltungsformate für Security Hub CSPM](#)
- [Konfiguration einer EventBridge Regel für Security Hub CSPM-Ergebnisse](#)
- [Verwenden von benutzerdefinierten Aktionen zum Senden von Ergebnissen und Erkenntnisergebnissen an EventBridge](#)

Security Hub CSPM-Ereignistypen in EventBridge

Security Hub CSPM verwendet die folgenden EventBridge Amazon-Ereignistypen für die Integration. EventBridge

Auf dem EventBridge Dashboard für Security Hub CSPM umfasst Alle Ereignisse all diese Ereignistypen.

Alle Funde (Security Hub Findings - Imported)

Security Hub CSPM sendet automatisch alle neuen Erkenntnisse und alle Aktualisierungen vorhandener Ergebnisse EventBridge als Security Hub Findings - ImportedEreignisse an. Jedes Security Hub Findings - ImportedEreignis enthält ein einzelnes Ergebnis.

Jede [BatchImportFindingsBatchUpdateFindings](#)AND-Anfrage löst ein Security Hub Findings - ImportedEreignis aus.

Bei Administratorkonten EventBridge enthält der Event-Feed Ereignisse für Ergebnisse sowohl aus ihrem Konto als auch aus ihren Mitgliedskonten.

In einer Aggregationsregion enthält der Event-Feed Ereignisse für Ergebnisse aus der Aggregationsregion und den verknüpften Regionen. Regionsübergreifende Ergebnisse werden nahezu in Echtzeit in den Event-Feed aufgenommen. Informationen zur Konfiguration der Suchaggregation finden Sie unter. [Aggregation von CSPM-Daten über Regionen hinweg](#)

Sie können Regeln definieren EventBridge , die Ergebnisse automatisch an einen Korrektur-Workflow, ein Drittanbieter-Tool oder ein [anderes unterstütztes EventBridge](#) Ziel weiterleiten. Die Regeln können Filter enthalten, die die Regel nur anwenden, wenn das Ergebnis bestimmte Attributwerte hat.

Sie verwenden diese Methode, um automatisch alle Ergebnisse oder alle Ergebnisse, die bestimmte Merkmale aufweisen, an einen Reaktions- oder Behebungsworkflow zu senden.

Siehe [the section called “Eine Regel konfigurieren EventBridge ”](#).

Funde für benutzerdefinierte Aktionen (Security Hub Findings - Custom Action)

Security Hub CSPM sendet auch Ergebnisse, die mit benutzerdefinierten Aktionen verknüpft sind, EventBridge als Security Hub Findings - Custom ActionEreignisse an.

Dies ist nützlich für Analysten, die mit der Security Hub CSPM-Konsole arbeiten und ein bestimmtes Ergebnis oder eine kleine Gruppe von Ergebnissen an einen Reaktions- oder Behebungsworkflow senden möchten. Sie können eine benutzerdefinierte Aktion für bis zu 20 Funde gleichzeitig auswählen. Jedes Ergebnis wird EventBridge als separates Ereignis gesendet. EventBridge

Wenn Sie eine benutzerdefinierte Aktion erstellen, weisen Sie ihr eine benutzerdefinierte Aktions-ID zu. Sie können diese ID verwenden, um eine EventBridge Regel zu erstellen, die eine bestimmte Aktion ausführt, nachdem sie ein Ergebnis erhalten hat, das mit dieser benutzerdefinierten Aktions-ID verknüpft ist.

Siehe [the section called “Konfiguration und Verwendung benutzerdefinierter Aktionen”](#).

Sie können beispielsweise eine benutzerdefinierte Aktion in Security Hub CSPM mit dem Namen `send_to_ticketing` erstellen. Anschließend erstellen Sie eine Regel EventBridge, die ausgelöst wird, wenn EventBridge ein Ergebnis eingeht, das die `send_to_ticketing` benutzerdefinierte Aktions-ID enthält. Die Regel beinhaltet eine Logik zum Senden der Funde an Ihr Ticketing-System. Anschließend können Sie Ergebnisse in Security Hub CSPM auswählen und die benutzerdefinierte Aktion in Security Hub CSPM verwenden, um Ergebnisse manuell an Ihr Ticketsystem zu senden.

Beispiele dafür, wie Sie CSPM-Ergebnisse von Security Hub EventBridge zur weiteren Verarbeitung an diese senden können, finden Sie unter [How to Integrate AWS Security Hub Cloud Security Posture Management \(CSPM\) Custom Actions with PagerDuty](#) and [How to Enable Custom Actions in AWS Security Hub Cloud Security Posture Management \(CSPM\) im AWS Partner Network \(APN\)](#) - Blog.

Insight-Ergebnisse für benutzerdefinierte Aktionen (Security Hub Insight Results)

Sie können auch benutzerdefinierte Aktionen verwenden, um Gruppen von Insight-Ergebnissen als Ereignisse an sie zu senden. EventBridge Security Hub Insight Results Insight-Ergebnisse sind die Ressourcen, die einem Einblick entsprechen. Beachten Sie, dass Sie, wenn Sie Insight-Ergebnisse an EventBridge senden, die Ergebnisse nicht an diese senden EventBridge. Sie senden nur die Ressourcen-IDs, die mit den Insight-Ergebnissen verknüpft sind. Sie können bis zu 100 Ressourcenkennungen gleichzeitig senden.

Ähnlich wie bei benutzerdefinierten Aktionen für Ergebnisse erstellen Sie zuerst die benutzerdefinierte Aktion in Security Hub CSPM und dann eine Regel in EventBridge.

Siehe [the section called “Konfiguration und Verwendung benutzerdefinierter Aktionen”](#).

Nehmen wir zum Beispiel an, Sie sehen ein bestimmtes Insight-Ergebnis von Interesse, das Sie mit einem Kollegen teilen möchten. In diesem Fall können Sie eine benutzerdefinierte Aktion verwenden, um dieses Insight-Ergebnis über ein Chat- oder Ticketsystem an den Kollegen zu senden.

EventBridge Veranstaltungsformate für Security Hub CSPM

Die Security Hub Insight Results Ereignistypen Security Hub Findings - Imported Security Findings - Custom Action, und verwenden die folgenden Veranstaltungsformate.

Das Ereignisformat ist das Format, das verwendet wird, wenn Security Hub CSPM ein Ereignis sendet. EventBridge

Security Hub Findings - Imported

Security Hub Findings - Imported Ereignisse, die von Security Hub CSPM gesendet werden, um das folgende EventBridge Format zu verwenden.

```
{
  "version": "0",
  "id": "CWE-event-id",
  "detail-type": "Security Hub Findings - Imported",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2019-04-11T21:52:17Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:securityhub:us-west-2::product/aws/macie/arn:aws:macie:us-west-2:111122223333:integtest/trigger/6294d71b927c41cbab915159a8f326a3/alert/f2893b211841"
  ],
  "detail": {
    "findings": [
      <finding content>
    ]
  }
}
```

<finding content> ist der Inhalt des Ergebnisses, das durch das Ereignis gesendet wird, im JSON-Format. Jedes Ereignis sendet einen einzelnen Befund.

Eine vollständige Liste der Suchattribute finden Sie unter [AWS Format für Sicherheitssuche \(ASFF\)](#).

Informationen zur Konfiguration von EventBridge Regeln, die durch diese Ereignisse ausgelöst werden, finden Sie unter [the section called “Eine Regel konfigurieren EventBridge”](#).

Security Hub Findings - Custom Action

Security Hub Findings - Custom Action Ereignisse, die von Security Hub CSPM gesendet werden, um das folgende EventBridge Format zu verwenden. Jeder Befund wird in einem separaten Ereignis gesendet.

```
{
  "version": "0",
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
```



```

"detail-type": "Security Hub Findings - Custom Action",
"source": "aws.securityhub",
"account": "111122223333",
"time": "2019-04-11T18:43:48Z",
"region": "us-west-1",
"resources": [
  "arn:aws:securityhub:us-west-1:111122223333:action/custom/custom-action-name"
],
"detail": {
  "actionName": "custom-action-name",
  "actionDescription": "description of the action",
  "findings": [
    {
      <finding content>
    }
  ]
}
}

```

<finding content> ist der Inhalt des Ergebnisses, das durch das Ereignis gesendet wird, im JSON-Format. Jedes Ereignis sendet einen einzelnen Befund.

Eine vollständige Liste der Suchattribute finden Sie unter [AWS Format für Sicherheitssuche \(ASFF\)](#).

Informationen zur Konfiguration von EventBridge Regeln, die durch diese Ereignisse ausgelöst werden, finden Sie unter [the section called “Konfiguration und Verwendung benutzerdefinierter Aktionen”](#).

Security Hub Insight Results

Security Hub Insight Results Ereignisse, die von Security Hub CSPM gesendet werden, um das folgende EventBridge Format zu verwenden.

```

{
  "version": "0",
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
  "detail-type": "Security Hub Insight Results",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-west-1",
  "resources": [

```

```

    "arn:aws:securityhub:us-west-1:111122223333::product/aws/maciek:us-west-1:222233334444:test/trigger/1ec9cf700ef6be062b19584e0b7d84ec/alert/f2893b211841"
  ],
  "detail": {
    "actionName": "name of the action",
    "actionDescription": "description of the action",
    "insightArn": "ARN of the insight",
    "insightName": "Name of the insight",
    "resultType": "ResourceAwsIamAccessKeyUserName",
    "number of results": "number of results, max of 100",
    "insightResults": [
      {"result 1": 5},
      {"result 2": 6}
    ]
  }
}

```

Informationen zum Erstellen einer EventBridge Regel, die durch diese Ereignisse ausgelöst wird, finden Sie unter [the section called “Konfiguration und Verwendung benutzerdefinierter Aktionen”](#)

Konfiguration einer EventBridge Regel für Security Hub CSPM-Ergebnisse

Sie können in Amazon eine Regel erstellen EventBridge , die eine Aktion definiert, die ausgeführt werden soll, wenn ein Security Hub Findings - ImportedEreignis eingeht. Security Hub Findings - ImportedEreignisse werden durch Aktualisierungen sowohl von den als auch von [BatchImportFindingsBatchUpdateFindings](#) Vorgängen ausgelöst.

Jede Regel enthält ein Ereignismuster, das die Ereignisse identifiziert, die die Regel auslösen. Das Ereignismuster enthält immer die Ereignisquelle (`aws.securityhub`) und den Ereignistyp (Security Hub Hub-Ergebnisse — Importiert). Das Ereignismuster kann auch Filter angeben, um die Ergebnisse zu identifizieren, für die die Regel gilt.

Die Ereignisregel identifiziert dann die Regelziele. Die Ziele sind die Aktionen, die ergriffen werden müssen, EventBridge wenn ein Ereignis aus Security Hub Findings — Imported eingeht und das Ergebnis den Filtern entspricht.

Die hier bereitgestellten Anweisungen verwenden die EventBridge Konsole. Wenn Sie die Konsole verwenden, EventBridge wird automatisch die erforderliche ressourcenbasierte Richtlinie erstellt, die das Schreiben in Amazon CloudWatch Logs ermöglicht EventBridge .

Sie können auch den [PutRule](#) Betrieb der EventBridge API verwenden. Wenn Sie jedoch die EventBridge API verwenden, müssen Sie die ressourcenbasierte Richtlinie erstellen. Informationen

zu den erforderlichen Richtlinien finden Sie unter [CloudWatch Logs-Berechtigungen](#) im EventBridge Amazon-Benutzerhandbuch.

Format des Ereignismusters

Das Format des Ereignismusters für Security Hub Findings — Importierte Ereignisse lautet wie folgt:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Imported"
  ],
  "detail": {
    "findings": {
      <attribute filter values>
    }
  }
}
```

- `source` identifiziert Security Hub CSPM als den Dienst, der das Ereignis generiert.
- `detail-type` identifiziert den Ereignistyp.
- `detail` ist optional und stellt die Filterwerte für das Ereignismuster bereit. Wenn das Ereignismuster kein `detail` Feld enthält, lösen alle Ergebnisse die Regel aus.

Sie können die Ergebnisse auf der Grundlage eines beliebigen Ergebnisattributs filtern. Für jedes Attribut geben Sie ein durch Kommas getrenntes Array mit einem oder mehreren Werten an.

```
"<attribute name>": [ "<value1>", "<value2>" ]
```

Wenn Sie mehr als einen Wert für ein Attribut angeben, werden diese Werte durch verknüpft. OR Ein Ergebnis entspricht dem Filter für ein einzelnes Attribut, wenn das Ergebnis einen der aufgelisteten Werte enthält. Wenn Sie beispielsweise `INFORMATIONAL` sowohl als auch `LOW` als Werte für `severityLabel` angeben, stimmt das Ergebnis überein, wenn es den Schweregrad entweder `INFORMATIONAL` oder `LOW` hat.

Die Attribute werden durch verknüpft AND. Ein Ergebnis stimmt überein, wenn es den Filterkriterien für alle angegebenen Attribute entspricht.

Wenn Sie einen Attributwert angeben, muss dieser die Position dieses Attributs innerhalb der ASFF-Struktur (AWS Security Finding Format) widerspiegeln.

 Tip

Wir empfehlen, beim Filtern von Kontrollergebnissen die [Felder `SecurityControlId` oder `SecurityControlArn` ASFF](#) als Filter zu verwenden und nicht `Title` oder `Description`. Letztere Felder können sich gelegentlich ändern, wohingegen die Kontroll-ID und der ARN statische Identifikatoren sind.

Im folgenden Beispiel stellt das Ereignismuster Filterwerte für `ProductArn` und `Severity.Label` bereit, sodass ein Ergebnis zutrifft, wenn es von Amazon Inspector generiert wurde und den Schweregrad entweder `INFORMATIONAL` oder `LOW` hat.

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Imported"
  ],
  "detail": {
    "findings": {
      "ProductArn": ["arn:aws:securityhub:us-east-1::product/aws/inspector"],
      "Severity": {
        "Label": ["INFORMATIONAL", "LOW"]
      }
    }
  }
}
```

Eine Ereignisregel erstellen

Sie können ein vordefiniertes oder ein benutzerdefiniertes Ereignismuster verwenden, um eine Regel in zu erstellen EventBridge. Wenn Sie ein vordefiniertes Muster auswählen, EventBridge wird automatisch `source` und ausgefüllt `detail-type`. EventBridge stellt außerdem Felder zur Angabe von Filterwerten für die folgenden Suchattribute bereit:

- `AwsAccountId`

- `Compliance.Status`
- `Criticality`
- `ProductArn`
- `RecordState`
- `ResourceId`
- `ResourceType`
- `Severity.Label`
- `Types`
- `Workflow.Status`

Um eine EventBridge Regel zu erstellen (Konsole)

1. Öffnen Sie die EventBridge Amazon-Konsole unter <https://console.aws.amazon.com/events/>.
2. Erstellen Sie mit den folgenden Werten eine EventBridge Regel, die das Auffinden von Ereignissen überwacht:
 - Bei Regeltyp wählen Sie Regel mit einem Ereignismuster aus.
 - Wählen Sie aus, wie das Ereignismuster erstellt werden soll.

Um das Ereignismuster zu erstellen mit...	Vorgehensweise	
Eine Vorlage	Wählen Sie im Abschnitt Ereignismuster die folgenden Optionen aus: • Als Event source (Ereignisquelle) wählen Sie AWS -Services aus. • Wählen Sie als AWS Service Security Hub. • Wählen Sie als Ereignistyp die Option Security Hub Findings — Importiert aus.	

Um das Ereignismuster zu erstellen mit...	Vorgehensweise	
	• (Optional) Fügen Sie Filterwerte hinzu, um die Regel spezifischer zu gestalten. Um die Regel beispielsweise auf Ergebnisse mit aktivem Datensatzstatus zu beschränken, wählen Sie für Spezifische Datensatzstatus die Option Aktiv aus.	

Um das Ereignismuster zu erstellen mit...	Vorgehensweise	
Ein benutzerdefiniertes Ereignismuster (Verwenden Sie ein benutzerdefiniertes Muster, wenn Sie Ergebnisse anhand von Attributen filtern möchten, die nicht in der EventBridge Konsole angezeigt werden.)	- Wählen Sie im Abschnitt Ereignismuster die Option Benutzerdefinierte Muster (JSON-Editor) aus, und fügen Sie dann das folgende Ereignismuster in den Textbereich ein: <pre>{ "source": ["aws.secu rityhub"], "detail-type": ["Security Hub Findings - Imported"], "detail": { "findings": { "<attribut e name> ": ["<value1>", "<value2>"] } } }</pre> - Aktualisieren Sie das Ereignismuster so, dass es die Attribut- und Attributwerte enthält, die Sie als Filter verwenden möchten. Verwenden Sie beispielsweise das folgende	

Um das Ereignismuster zu erstellen mit...	Vorgehensweise	
	Musterbeispiel, um die Regel auf Ergebnisse anzuwenden TRUE_POSITIVE, die den Bestätigungsstatus haben: <pre data-bbox="690 520 1062 1276"> { "source": ["aws.securityhub"], "detail-type": ["Security Hub Findings - Imported"], "detail": { "findings": { "VerificationState": ["TRUE_POSITIVE"] } } }</pre>	

- Wählen Sie für Zieltypen die Option AWS Service und für Ziel auswählen ein Ziel aus, z. B. ein Amazon SNS-Thema oder eine Amazon AWS Lambda SNS-Funktion. Das Ziel wird ausgelöst, wenn ein Ereignis empfangen wird, das dem in der Regel definierten Ereignismuster entspricht.

Einzelheiten zum Erstellen von Regeln finden Sie im [EventBridge Amazon-Benutzerhandbuch unter Erstellen von EventBridge Amazon-Regeln, die auf Ereignisse reagieren](#).

Verwenden von benutzerdefinierten Aktionen zum Senden von Ergebnissen und Erkenntnisergebnissen an EventBridge

Um benutzerdefinierte Aktionen von AWS Security Hub Cloud Security Posture Management (CSPM) zu verwenden, um Ergebnisse oder Insight-Ergebnisse an Amazon zu senden EventBridge, erstellen Sie zunächst die benutzerdefinierte Aktion in Security Hub CSPM. Anschließend können Sie Regeln definieren, die für Ihre EventBridge benutzerdefinierten Aktionen gelten.

Sie können bis zu 50 benutzerdefinierte Aktionen erstellen.

Wenn Sie die regionsübergreifende Aggregation aktivieren und Ergebnisse aus der Aggregationsregion verwalten, erstellen Sie benutzerdefinierte Aktionen in der Aggregationsregion.

Die Regel EventBridge verwendet den Amazon-Ressourcennamen (ARN) aus der benutzerdefinierten Aktion.

Eine benutzerdefinierte Aktion erstellen

Wenn Sie eine benutzerdefinierte Aktion in AWS Security Hub Cloud Security Posture Management (CSPM) erstellen, geben Sie deren Namen, Beschreibung und eine eindeutige Kennung an.

Eine benutzerdefinierte Aktion gibt an, welche Aktionen ausgeführt werden sollen, wenn ein EventBridge Ereignis einer EventBridge Regel entspricht. Security Hub CSPM sendet jedes Ergebnis EventBridge als Ereignis an.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um eine benutzerdefinierte Aktion zu erstellen.

Console

Um eine benutzerdefinierte Aktion in Security Hub CSPM (Konsole) zu erstellen

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Settings (Einstellungen) und dann Custom actions (Benutzerdefinierte Aktionen) aus.
3. Wählen Sie Create custom action (Benutzerdefinierte Aktion erstellen) aus.
4. Machen Sie für die Aktion Angaben bei Name, Description (Beschreibung) und Custom action ID (Benutzerdefinierte Aktions-ID).

Der Name muss weniger als 20 Zeichen lang sein.

Die benutzerdefinierte Aktions-ID muss für jedes AWS Konto eindeutig sein.

5. Wählen Sie **Create custom action** (Benutzerdefinierte Aktion erstellen) aus.
6. Notieren Sie sich den Custom action ARN (Benutzerdefinierter Aktions-ARN). Sie müssen den ARN verwenden, wenn Sie eine Regel erstellen, um sie in EventBridge dieser Aktion zuzuordnen.

API

Um eine benutzerdefinierte Aktion (API) zu erstellen

Verwenden Sie die [CreateActionTarget](#) Operation. Wenn Sie den verwenden AWS CLI, führen Sie den [create-action-target](#) Befehl aus.

Im folgenden Beispiel wird eine benutzerdefinierte Aktion erstellt, um Ergebnisse an ein Behebungstool zu senden. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub create-action-target --name "Send to remediation" --description "Action to send the finding for remediation tracking" --id "Remediation"
```

Definition einer Regel in EventBridge

Um eine benutzerdefinierte Aktion in Amazon auszulösen EventBridge, müssen Sie eine entsprechende Regel in erstellen EventBridge. Die Regeldefinition beinhaltet den Amazon-Ressourcennamen (ARN) der benutzerdefinierten Aktion.

Das Ereignismuster für ein Security Hub Findings — Custom Action-Ereignis hat das folgende Format:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Custom Action"
  ],
```

```
"resources": [ "<custom action ARN>" ]
}
```

Das Ereignismuster für ein Security Hub Insight Results-Ereignis hat das folgende Format:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Insight Results"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

In beiden Mustern *<custom action ARN>* ist dies der ARN einer benutzerdefinierten Aktion. Sie können eine Regel konfigurieren, die für mehr als eine benutzerdefinierte Aktion gilt.

Die hier bereitgestellten Anweisungen gelten für die EventBridge Konsole. Wenn Sie die Konsole verwenden, EventBridge wird automatisch die erforderliche ressourcenbasierte Richtlinie erstellt, die das Schreiben EventBridge in Protokolle ermöglicht. CloudWatch

Sie können auch den [PutRule](#)API-Betrieb der EventBridge API verwenden. Wenn Sie jedoch die EventBridge API verwenden, müssen Sie die ressourcenbasierte Richtlinie erstellen. Einzelheiten zu den erforderlichen Richtlinien finden Sie unter [CloudWatch Logs-Berechtigungen](#) im EventBridge Amazon-Benutzerhandbuch.

Um eine Regel in EventBridge (EventBridge Konsole) zu definieren

1. Öffnen Sie die EventBridge Amazon-Konsole unter <https://console.aws.amazon.com/events/>.
2. Wählen Sie im Navigationsbereich Regeln aus.
3. Wählen Sie Regel erstellen aus.
4. Geben Sie einen Namen und eine Beschreibung für die Regel ein.
5. Wählen Sie für Event Bus den Event Bus aus, den Sie dieser Regel zuordnen möchten. Wenn Sie möchten, dass diese Regel mit Ereignissen aus Ihrem eigenen Konto übereinstimmt, wählen Sie Standard aus. Wenn ein AWS -Service in Ihrem Konto ein Ereignis ausgibt, wird es stets an den Standard-Event-Bus Ihres Kontos weitergeleitet.
6. Bei Regeltyp wählen Sie Regel mit einem Ereignismuster aus.

7. Wählen Sie Weiter aus.
8. Wählen Sie unter Event source (Ereignisquelle) AWS events (Ereignisse) aus.
9. Wählen Sie für Ereignismuster die Option Ereignismusterformular.
10. Als Event source (Ereignisquelle) wählen Sie AWS -Services aus.
11. Wählen Sie als AWS Service Security Hub.
12. Führen Sie für Type (Typ) eine der folgenden Aktionen aus:
 - Um eine Regel zu erstellen, die angewendet wird, wenn Sie Ergebnisse an eine benutzerdefinierte Aktion senden, wählen Sie Security Hub Hub-Ergebnisse — Benutzerdefinierte Aktion.
 - Um eine Regel zu erstellen, die angewendet wird, wenn Sie Insight-Ergebnisse an eine benutzerdefinierte Aktion senden, wählen Sie Security Hub Insight-Ergebnisse.
13. Wählen Sie Spezifische benutzerdefinierte Aktion ARNs und fügen Sie einen benutzerdefinierten Aktions-ARN hinzu.

Wenn die Regel für mehrere benutzerdefinierte Aktionen gilt, wählen Sie Hinzufügen aus, um weitere benutzerdefinierte Aktionen hinzuzufügen ARNs.

14. Wählen Sie Weiter aus.
15. Wählen und konfigurieren Sie unter Ziele auswählen das Ziel, das aufgerufen werden soll, wenn diese Regel erfüllt ist.
16. Wählen Sie Weiter aus.
17. (Optional) Geben Sie ein oder mehrere Tags für die Regel ein. Weitere Informationen finden Sie unter [EventBridge Amazon-Tags](#) im EventBridge Amazon-Benutzerhandbuch.
18. Wählen Sie Weiter aus.
19. Überprüfen Sie die Details der Regel und wählen Sie dann Regel erstellen aus.

Wenn Sie eine benutzerdefinierte Aktion mit Ergebnissen oder Insight-Ergebnissen in Ihrem Konto durchführen, werden Ereignisse in generiert EventBridge.

Auswahl einer benutzerdefinierten Aktion für Ergebnisse und Insight-Ergebnisse

Nachdem Sie benutzerdefinierte Aktionen und EventBridge Amazon-Regeln für AWS Security Hub Cloud Security Posture Management (CSPM) erstellt haben, können Sie Ergebnisse und Insight-Ergebnisse EventBridge zur automatischen Verwaltung und Verarbeitung an diese senden.

Ereignisse werden EventBridge nur an das Konto gesendet, in dem sie angesehen werden. Wenn Sie ein Ergebnis mit einem Administratorkonto anzeigen, wird das Ereignis EventBridge an das Administratorkonto gesendet.

Damit AWS API-Aufrufe wirksam sind, müssen bei den Implementierungen des Zielcodes Rollen in Mitgliedskonten umgewandelt werden. Das bedeutet auch, dass die Rolle, in die Sie wechseln, für jedes Mitglied bereitgestellt werden muss, bei dem Maßnahmen erforderlich sind.

Um Ergebnisse an EventBridge (Konsole) zu senden

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>
2. Zeigen Sie eine Liste der Ergebnisse an:
 - Unter Ergebnisse können Sie die Ergebnisse aller aktivierten Produktintegrationen und Kontrollen einsehen.
 - Unter Sicherheitsstandards können Sie zu einer Liste mit Ergebnissen navigieren, die anhand einer bestimmten Kontrolle generiert wurden. Weitere Informationen finden Sie unter [Überprüfung der Details der Kontrollen in Security Hub CSPM](#).
 - Unter Integrationen können Sie zu einer Liste von Ergebnissen navigieren, die durch eine aktivierte Integration generiert wurden. Weitere Informationen finden Sie unter [Ergebnisse einer Security Hub CSPM-Integration anzeigen](#).
 - In Insights können Sie zu einer Ergebnisliste für ein Insight-Ergebnis navigieren. Weitere Informationen finden Sie unter [Überprüfung und Umsetzung von Erkenntnissen in Security Hub CSPM](#).
3. Wählen Sie die Ergebnisse aus, an die Sie senden möchten EventBridge. Sie können bis zu 20 Ergebnisse gleichzeitig auswählen.
4. Wählen Sie unter Aktionen die benutzerdefinierte Aktion aus, die der anzuwendenden EventBridge Regel entspricht.

Security Hub CSPM sendet für jeden Befund ein separates Ereignis Security Hub Findings — Custom Action.

Um Insight-Ergebnisse an EventBridge (Konsole) zu senden

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>

2. Wählen Sie im Navigationsbereich **Insights** aus.
3. Wählen Sie auf der Seite **Insights** den **Insight** aus, der die Ergebnisse enthält, an die Sie senden möchten. **EventBridge**
4. Wählen Sie die **Insight-Ergebnisse** aus, an die Sie senden möchten **EventBridge**. Sie können bis zu 20 Ergebnisse gleichzeitig auswählen.
5. Wählen Sie unter **Aktionen** die benutzerdefinierte Aktion aus, die der anzuwendenden **EventBridge Regel** entspricht.

Arbeiten mit dem Dashboard in Security Hub CSPM

Auf der Übersichtsseite in der Security Hub Hub-Konsole wird eine Zusammenfassung Ihrer Risiken, Angriffssequenzen und Sicherheitsvorkehrungen angezeigt. Auf dieser Seite können Sie Risiken und Angriffssequenzen anhand ihres Schweregrads und der Kontoabdeckung für verschiedene Sicherheitsfunktionen identifizieren. Sie können diese Seite anpassen, indem Sie verschiedene Sicherheits-Widgets hinzufügen und entfernen und Filterkriterien für den Abruf bestimmter Datentypen festlegen.

Anpassungen an dieser Seite werden für die future Verwendung gespeichert. Wenn Benutzer in Ihrem Konto diese Seite anpassen, werden ihre Anpassungseinstellungen unabhängig von Ihren Anpassungseinstellungen gespeichert.

Wenn es sich bei Ihrem Konto um das delegierte Administratorkonto für eine Organisation handelt, umfassen die Daten auch Ergebnisse für Ihr Konto und Ihre Mitgliedskonten. Wenn es sich bei Ihrem Konto um ein Mitgliedskonto oder ein eigenständiges Konto handelt, enthalten die Daten nur Ergebnisse für Ihr Konto.

Wenn Sie die regionsübergreifende Aggregation in Security Hub CSPM konfigurieren, werden auf dieser Seite die Ergebnisse Ihrer Aggregation angezeigt

Note

Jedes Mal, wenn Sie diese Seite öffnen, wird sie automatisch aktualisiert.
Sicherheitsbewertungen und Kontrollstatus werden jedoch alle 24 Stunden aktualisiert.

Das Widget mit der Risikoübersicht

Dieses Widget zeigt alle Ihre Risiken nach Schweregrad an. Risiken mit höherem Schweregrad werden zuerst angezeigt. Die Risiken basieren auf einer Analyse der Ergebnisse und Merkmale von Security Hub CSPM und anderen AWS-Services

Das Widget mit der Zusammenfassung der Bedrohungen

Dieses Widget zeigt alle Ihre Angriffssequenzen nach Schweregrad an. Angriffssequenzen mit höherem Schweregrad werden zuerst angezeigt. Angriffssequenzen beziehen sich auf eine Reihe

von Ereignissen und identifizieren potenzielle Bedrohungen in Ihrer Umgebung. Sie haben auch ihren Ursprung in GuardDuty.

Das Widget zur Sicherheitsabdeckung

Verfügbare Widgets für das Übersichts-Dashboard

Das Übersichts-Dashboard enthält Widgets, die die aktuelle Bedrohungslandschaft der Cloud-Sicherheit widerspiegeln und sich dabei an den Sicherheitsabläufen und Erfahrungen der AWS Kunden orientieren. Einige Widgets werden standardmäßig angezeigt, andere nicht. Sie können Ihre Ansicht des Dashboards anpassen, indem Sie Widgets hinzufügen oder entfernen.

Um sie hinzuzufügen, wählen Sie oben rechts auf der Übersichtsseite Widget hinzufügen. Geben Sie in der Suchleiste den Titel des Widgets ein. Ziehen Sie das Widget per Drag & Drop auf das Dashboard.

Standardmäßig werden Widgets angezeigt

Standardmäßig enthält das Übersichts-Dashboard die folgenden Widgets:

Sequenzen der wichtigsten Bedrohungen

Zeigt die Bedrohungssequenzen mit dem höchsten Schweregrad an. Die Ergebnisse der Bedrohungssequenz, bei Amazon als Ergebnisse der Angriffssequenz bekannt GuardDuty, korrelieren mehrere Ereignisse, um potenzielle Bedrohungen für Ihre AWS Umgebung zu identifizieren. Zu den Bedrohungssequenzen können aktuelle oder kürzlich aufgetretene Angriffe (innerhalb eines 24-Stunden-Zeitfensters) in Ihrer Umgebung gehören, die wiederum zu weiteren Bedrohungen führen können. Sie müssen GuardDuty S3-Schutz aktiviert haben GuardDuty , um Ergebnisse der Bedrohungssequenz in Security Hub CSPM empfangen zu können.

Die größten Risiken

Zeigt eine Zusammenfassung der wichtigsten Risiken in Ihrer Umgebung an. Im oberen Bereich des Widgets wird die Anzahl der Risiken für jeden Schweregrad angezeigt. Sie können einen Schweregrad auswählen, um zur Seite Risiken zu gelangen, auf der die Risiken nach dem ausgewählten Schweregrad gefiltert werden. Die Risiken, die in Ihrer Umgebung am häufigsten vorkommen, werden zuerst angezeigt. Dieses Widget hilft Ihnen bei der Priorisierung der Risiken, die gemindert werden müssen.

Sicherheitsabdeckung

Fasst den Umfang Ihres Sicherheitsschutzes auf der Grundlage der Ergebnisse der Deckungskontrolle zusammen. Bei der Deckungskontrolle wird geprüft, ob ein bestimmtes Objekt AWS-Service und seine Funktionen aktiviert sind (z. B. [\[Macie.1\] Amazon Macie sollte aktiviert sein](#)). Mit diesem Widget können Sie sicherstellen, dass Sie über PASSED Ergebnisse für die Deckungskontrolle verfügen. Die Security Hub CSPM-Konsole bietet Links aus diesem Widget, mit denen Sie fehlende Sicherheitsfunktionen aktivieren können. Wir empfehlen, die zentrale Konfiguration zu verwenden, um fehlende Sicherheitsfunktionen für mehrere AWS-Konten und zu aktivieren. AWS-Regionen Weitere Informationen finden Sie unter [Grundlegendes zur zentralen Konfiguration in Security Hub CSPM](#).

Sicherheitsstandards

Zeigt Ihre aktuelle zusammenfassende Sicherheitsbewertung und die Sicherheitsbewertung für jeden Security Hub CSPM-Standard an. Sicherheitswerte, die zwischen 0 und 100 Prozent liegen, stellen den Anteil der bestandenen Kontrollen im Verhältnis zu all Ihren aktivierten Kontrollen dar. Weitere Informationen zu diesen Bewertungen finden Sie unter [Methode zur Berechnung von Sicherheitswerten](#). Dieses Widget hilft Ihnen dabei, Ihren allgemeinen Sicherheitsstatus zu verstehen.

Sicherheitsstandards

Zeigt Ihre aktuelle zusammenfassende Sicherheitsbewertung und die Sicherheitsbewertung für jeden Security Hub CSPM-Standard an. Sicherheitswerte, die zwischen 0 und 100 Prozent liegen, stellen den Anteil der bestandenen Kontrollen im Verhältnis zu all Ihren aktivierten Kontrollen dar. Weitere Informationen zu diesen Bewertungen finden Sie unter [Methode zur Berechnung von Sicherheitswerten](#). Dieses Widget hilft Ihnen dabei, Ihren allgemeinen Sicherheitsstatus zu verstehen.

Anlagen mit den meisten Ergebnissen

Bietet einen Überblick über die Ressourcen, Konten und Anwendungen, die die meisten Ergebnisse erzielt haben. Die Liste ist in absteigender Reihenfolge nach der Anzahl der Ergebnisse sortiert. Im Widget zeigt jede Registerkarte die sechs wichtigsten Elemente in dieser Kategorie, gruppiert nach Schweregrad und Ressourcentyp. Wenn Sie in der Spalte Ergebnisse insgesamt eine Zahl auswählen, öffnet Security Hub CSPM eine Seite, auf der die Ergebnisse für das Asset angezeigt werden. Mit diesem Widget können Sie schnell erkennen, welche Ihrer Kernressourcen potenzielle Sicherheitsbedrohungen bergen.

Ergebnisse nach Regionen

Zeigt die Gesamtzahl der Ergebnisse, gruppiert nach Schweregrad, in jedem Fall an, AWS-Region in dem Security Hub CSPM aktiviert ist. Dieses Widget hilft Ihnen dabei, Sicherheitsprobleme zu identifizieren, die möglicherweise bestimmte Regionen betreffen. Wenn Sie das Dashboard in Ihrer Aggregationsregion öffnen, hilft Ihnen dieses Widget dabei, potenzielle Sicherheitsprobleme in jeder verknüpften Region zu überwachen.

Die häufigsten Bedrohungsarten

Bietet eine Aufschlüsselung der 10 häufigsten Bedrohungstypen in Ihrer AWS Umgebung. Dazu gehören Bedrohungen wie die Eskalation von Rechten, die Verwendung offengelegter Anmeldeinformationen oder die Kommunikation mit bösartigen IP-Adressen.

Um diese Daten anzeigen zu können, GuardDuty muss [Amazon](#) aktiviert sein. Wenn ja, wählen Sie in diesem Widget einen Bedrohungstyp aus, um die GuardDuty Konsole zu öffnen und die Ergebnisse zu dieser Bedrohung zu überprüfen. Dieses Widget hilft Ihnen dabei, potenzielle Bedrohungen im Zusammenhang mit anderen Sicherheitsproblemen zu bewerten.

Sicherheitslücken in Software durch Exploits

Bietet eine Zusammenfassung der Softwareschwachstellen, die in Ihrer AWS Umgebung bestehen und für die bereits bekannte Exploits vorliegen. Sie können sich auch eine Aufschlüsselung der Sicherheitslücken ansehen, für die es Lösungen gibt und für die es keine gibt.

Um diese Daten anzeigen zu können, muss [Amazon Inspector](#) aktiviert sein. Wenn ja, wählen Sie eine Statistik in diesem Widget aus, um die Amazon Inspector Inspector-Konsole zu öffnen und weitere Details zu der Sicherheitslücke zu überprüfen. Dieses Widget hilft Ihnen dabei, Softwareschwachstellen im Zusammenhang mit anderen Sicherheitsproblemen zu bewerten.

Neue Erkenntnisse im Laufe der Zeit

Zeigt Trends bei der Anzahl neuer täglicher Ergebnisse in den letzten 90 Tagen. Sie können die Daten nach Schweregrad oder nach Anbieter aufschlüsseln, um zusätzlichen Kontext zu erhalten. Mithilfe dieses Widgets können Sie nachvollziehen, ob das gefundene Volumen in den letzten 90 Tagen zu bestimmten Zeiten angestiegen oder gesunken ist.

Ressourcen mit den meisten Ergebnissen

Bietet eine Zusammenfassung der Ressourcen, die zu den meisten Ergebnissen geführt haben, aufgeschlüsselt nach den folgenden Ressourcentypen: Amazon Simple Storage Service (Amazon

S3) -Buckets, Amazon Elastic Compute Cloud (Amazon EC2) -Instances und AWS Lambda Funktionen.

Im Widget konzentriert sich jede Registerkarte auf einen der vorherigen Ressourcentypen und listet die 10 Ressourcen-Instances auf, die die meisten Ergebnisse generiert haben. Um die Ergebnisse für eine bestimmte Ressource zu überprüfen, wählen Sie die Ressourceninstanz aus. Dieses Widget hilft Ihnen bei der Suche nach Sicherheitsergebnissen, die mit gängigen AWS Ressourcen verknüpft sind.

Widgets sind standardmäßig ausgeblendet

Die folgenden Widgets sind auch für das Übersichts-Dashboard verfügbar, sie sind jedoch standardmäßig ausgeblendet:

AMIs mit den meisten Ergebnissen

Stellt eine Liste der 10 Amazon Machine Images (AMIs) bereit, die die meisten Ergebnisse generiert haben. Diese Daten sind nur verfügbar, wenn Amazon sie für Ihr Konto EC2 aktiviert hat. Auf diese Weise können Sie erkennen, welche potenzielle Sicherheitsrisiken AMIs darstellen.

IAM-Prinzipale mit den meisten Ergebnissen

Stellt eine Liste der 10 AWS Identity and Access Management (IAM) -Benutzer bereit, die die meisten Ergebnisse generiert haben. Dieses Widget hilft Ihnen bei der Ausführung von Verwaltungs- und Abrechnungsaufgaben. Es zeigt Ihnen, welche Benutzer am meisten zur Nutzung von Security Hub CSPM beitragen.

Konten mit den meisten Ergebnissen (nach Schweregrad)

Zeigt eine grafische Darstellung der 10 Konten, die die meisten Ergebnisse generiert haben, gruppiert nach Schweregrad. Mithilfe dieses Widgets können Sie bestimmen, auf welche Konten Sie sich bei der Analyse und Problembehebung konzentrieren sollten.

Konten mit den meisten Ergebnissen (nach Ressourcentyp)

Zeigt ein Diagramm der 10 Konten, die die meisten Ergebnisse generiert haben, gruppiert nach Ressourcentyp. Mit diesem Widget können Sie bestimmen, welche Konten und Ressourcentypen für die Analyse und Problembehebung priorisiert werden müssen.

Einblicke

Führt fünf von [Security Hub CSPM verwaltete Erkenntnisse](#) und die Anzahl der Ergebnisse auf, die sie generiert haben. Insights identifizieren einen bestimmten Sicherheitsbereich, der Aufmerksamkeit erfordert.

Aktuelle Erkenntnisse aus AWS Integrationen

[Zeigt die Anzahl der Ergebnisse an, die Sie in Security Hub CSPM von integrated erhalten haben. AWS-Services](#) Außerdem wird angezeigt, wann Sie zuletzt Ergebnisse von den einzelnen integrierten Diensten erhalten haben. Dieses Widget bietet konsolidierte Ergebnisdaten aus mehreren AWS-Services. Wählen Sie einen integrierten Service aus, um weitere Informationen zu erhalten. Security Hub CSPM öffnet dann die Konsole für diesen Dienst.

Filtern des Übersichts-Dashboards in Security Hub CSPM

Sie können das Übersichts-Dashboard auf der AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole so verwalten, dass es nur die Sicherheitsdaten enthält, die für Sie am relevantesten sind. Wenn Sie beispielsweise Mitglied eines Anwendungsteams sind, können Sie eine spezielle Ansicht für eine wichtige Anwendung in Ihrer Produktionsumgebung erstellen. Wenn Sie Mitglied eines Sicherheitsteams sind, können Sie eine spezielle Ansicht erstellen, die Ihnen hilft, sich auf Ergebnisse mit hohem Schweregrad zu konzentrieren.

Um diese kuratierten Ansichten zu erstellen, geben Sie Filterkriterien in das Filterfeld über dem Dashboard ein. Wenn Sie Filterkriterien anwenden, gelten die Kriterien für alle Daten und Widgets im Dashboard, mit Ausnahme der Daten in den Widgets Einblicke und Sicherheitsstandards. Eine Liste der verfügbaren Widgets auf dem Dashboard finden Sie unter [Verfügbare Widgets für das Übersichts-Dashboard](#).

Sie können die Daten mithilfe der folgenden Felder filtern:

- Account name (Kontoname)
- Konto-ID
- Amazon-Ressourcenname (ARN) der Anwendung
- Anwendungsname
- Produktname (für ein Produkt AWS-Service oder ein Produkt eines Drittanbieters, das Ergebnisse an Security Hub CSPM sendet)
- Record state (Datensatzstatus)

- Region
- Ressourcen-Tag
- Schweregrad
- Workflow-Status

Standardmäßig werden Dashboard-Daten anhand der folgenden Kriterien gefiltert:

`Workflow.Status` ist NOTIFIED oder NEW, und `RecordState` ist ACTIVE. Diese Kriterien werden über dem Dashboard unter dem Filterfeld angezeigt. Um diese Kriterien zu entfernen, wählen Sie X im Filtertoken für die Kriterien, die Sie entfernen möchten.

Wenn Sie Filterkriterien anwenden, die Sie erneut verwenden möchten, können Sie sie als Filtersatz speichern. Ein Filtersatz besteht aus einer Reihe von Filterkriterien, die Sie erstellen und speichern, um sie erneut anzuwenden, wenn Sie Daten im Übersichts-Dashboard überprüfen.

Note

Die folgenden Felder können nicht als Teil eines Filtersatzes gespeichert werden:
Anwendungs-ARN, Anwendungsname und Ressourcen-Tag.

Filtersätze erstellen und speichern

Gehen Sie wie folgt vor, um einen Filtersatz zu erstellen und zu speichern.

Um einen Filtersatz zu erstellen und zu speichern

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Zusammenfassung aus.
3. Geben Sie im Filterfeld über dem Übersichts-Dashboard die Filterkriterien für den Filtersatz ein.
4. Wählen Sie im Menü Filter löschen die Option Neuen Filtersatz speichern aus.
5. Geben Sie im Dialogfeld Filtersatz speichern einen Namen für den Filtersatz ein.
6. (Optional) Um den Filtersatz bei jedem Öffnen der Übersichtsseite standardmäßig zu verwenden, wählen Sie die Option, um ihn als Standardansicht festzulegen.
7. Wählen Sie Speichern.

Um zwischen den von Ihnen erstellten und gespeicherten Filtersätzen zu wechseln, verwenden Sie das Menü „Filtersatz auswählen“ über dem Übersichts-Dashboard. Wenn Sie einen Filtersatz auswählen, wendet Security Hub CSPM die Kriterien des Filtersatzes auf die Daten im Dashboard an.

Filtersätze aktualisieren oder löschen

Gehen Sie wie folgt vor, um einen vorhandenen Filtersatz zu aktualisieren oder zu löschen. Wenn Sie einen Filtersatz löschen, der derzeit als Standardansicht des Übersichts-Dashboards eingerichtet ist, wird Ihre Standardansicht auf die Standardansicht von Security Hub CSPM zurückgesetzt.

Um einen Filtersatz zu aktualisieren oder zu löschen

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Zusammenfassung aus.
3. Wählen Sie im Menü Wählen Sie einen Filtersatz über der Übersichtsseite den Filtersatz aus.
4. Führen Sie im Menü Filter löschen einen der folgenden Schritte aus:
 - Um den Filtersatz zu aktualisieren, wählen Sie Aktuellen Filtersatz aktualisieren. Geben Sie dann Ihre Änderungen in das angezeigte Dialogfeld ein.
 - Um den Filtersatz zu löschen, wählen Sie Aktuellen Filtersatz löschen. Wählen Sie anschließend im daraufhin angezeigten Dialogfeld die Option Löschen.

Anpassen des Übersichts-Dashboards in Security Hub CSPM

Sie können das Übersichts-Dashboard auf der AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole auf verschiedene Arten anpassen. Sie können zum Beispiel Widgets zum Dashboard hinzufügen und daraus entfernen. Sie können Widgets im Dashboard auch neu anordnen und ihre Größe ändern. Eine Liste der verfügbaren Widgets auf dem Dashboard finden Sie unter [Verfügbare Widgets für das Übersichts-Dashboard](#)

Wenn Sie das Dashboard anpassen, wendet Security Hub CSPM Ihre Änderungen sofort an und speichert Ihre neuen Dashboard-Einstellungen. Ihre Änderungen gelten für Ihre Ansicht des Dashboards in allen AWS-Regionen Browsern.

Um das Übersichts-Dashboard anzupassen

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter <https://console.aws.amazon.com/securityhub/>
2. Wählen Sie im Navigationsbereich Zusammenfassung aus.
3. Führen Sie eine der folgenden Aktionen aus:
 - Um ein Widget hinzuzufügen, wählen Sie in der oberen rechten Ecke der Seite Widgets hinzufügen. Geben Sie in der Suchleiste den Titel des Widgets ein, das Sie hinzufügen möchten. Ziehen Sie dann das Widget an die gewünschte Position.
 - Um ein Widget zu entfernen, wählen Sie die drei Punkte in der oberen rechten Ecke des Widgets aus.
 - Um ein Widget zu verschieben, wählen Sie den Ziehpunkt in der oberen linken Ecke des Widgets aus und ziehen Sie das Widget dann an die gewünschte Position.
 - Um die Größe eines Widgets zu ändern, wählen Sie den Ziehpunkt zur Größenänderung in der unteren rechten Ecke des Widgets. Ziehen Sie den Rand des Widgets, bis das Widget Ihre bevorzugte Größe hat.

Um anschließend die ursprünglichen Einstellungen wiederherzustellen, wählen Sie „Auf Standardlayout zurücksetzen“ oben auf der Seite.

Regionale Grenzwerte für Security Hub CSPM

Einige Funktionen von AWS Security Hub Cloud Security Posture Management (CSPM) sind nur in bestimmten Fällen verfügbar. AWS-Regionen In den folgenden Abschnitten werden diese regionalen Beschränkungen beschrieben. Eine vollständige Liste aller Regionen, in denen Security Hub CSPM derzeit verfügbar ist, finden Sie unter [AWS Security Hub Hub-Endpunkte und Kontingente](#) in der. Allgemeine AWS-Referenz

Regionsübergreifende Aggregationsbeschränkungen

In AWS GovCloud (US) Regions ist die [regionsübergreifende Aggregation](#) nur für Ergebnisse, Suchaktualisierungen und Erkenntnisse verfügbar. AWS GovCloud (US) Regions Insbesondere können Sie Ergebnisse, Aktualisierungen und Erkenntnisse nur zwischen den Regionen AWS GovCloud (USA-Ost) und AWS GovCloud (US-West) zusammenfassen.

In den China Regionen ist die regionsübergreifende Aggregation nur für Ergebnisse, Aktualisierungen und Einblicke in die Regionen China verfügbar. Insbesondere können Sie Ergebnisse, Aktualisierungen und Erkenntnisse nur zwischen den Regionen China (Peking) und China (Ningxia) zusammenfassen.

Sie können eine Region, die standardmäßig deaktiviert ist, nicht als Ihre Aggregationsregion verwenden. Eine Liste der Regionen, die standardmäßig deaktiviert sind, finden Sie im AWS -Kontenverwaltung Referenzhandbuch unter [AWS-Regionen In Ihrem Konto aktivieren oder deaktivieren](#).

Verfügbarkeit von Integrationen nach Regionen

Einige Integrationen sind nicht in allen verfügbar. AWS-Regionen Auf der Security Hub CSPM-Konsole wird eine Integration nicht auf der Seite Integrationen angezeigt, wenn sie in der Region, in der Sie derzeit angemeldet sind, nicht verfügbar ist.

Unterstützte Integrationen in den Regionen China (Peking) und China (Ningxia)

[In den Regionen China \(Peking\) und China \(Ningxia\) unterstützt Security Hub CSPM nur die folgenden Integrationen mit: AWS-Services](#)

- AWS Firewall Manager
- Amazon GuardDuty
- AWS Identity and Access Management Access Analyzer
- Amazon Inspector
- AWS IoT Device Defender
- AWS Systems Manager Explorer
- AWS Systems Manager OpsCenter
- AWS Systems Manager Patch-Manager

In den Regionen China (Peking) und China (Ningxia) unterstützt Security Hub CSPM nur die folgenden Integrationen von Drittanbietern:

- Cloud Custodian
- FireEye Helix
- Helecloud
- IBM QRadar
- PagerDuty
- Palo Alto Networks Cortex XSOAR
- Palo Alto Networks VM-Series
- Prowler
- RSA Archer
- Splunk Enterprise
- Splunk Phantom
- ThreatModeler

Integrationen werden in den Regionen AWS GovCloud (USA-Ost) und (US-West) unterstützt AWS GovCloud

In den Regionen AWS GovCloud (USA-Ost) und AWS GovCloud (US-West) unterstützt Security Hub CSPM nur die folgenden Integrationen mit: AWS-Services

- AWS Config

- Amazon Detective
- AWS Firewall Manager
- Amazon GuardDuty
- AWS Health
- IAM Access Analyzer
- Amazon Inspector
- AWS IoT Device Defender

In den Regionen AWS GovCloud (USA-Ost) und AWS GovCloud (US-West) unterstützt Security Hub CSPM nur die folgenden Integrationen von Drittanbietern:

- Atlassian Jira Service Management
- Atlassian Jira Service Management Cloud
- Atlassian OpsGenie
- Caveonix Cloud
- Cloud Custodian
- Cloud Storage Security Antivirus for Amazon S3
- CrowdStrike Falcon
- FireEye Helix
- Forcepoint CASB
- Forcepoint DLP
- Forcepoint NGFW
- Fugue
- Kion
- MicroFocus ArcSight
- NETSCOUT Cyber Investigator
- PagerDuty
- Palo Alto Networks – Prisma Cloud Compute
- Palo Alto Networks – Prisma Cloud Enterprise
- Palo Alto Networks – VM-Series(nur in AWS GovCloud (US-West) verfügbar)

- Prowler
- Rackspace Technology – Cloud Native Security
- Rapid7 InsightConnect
- RSA Archer
- SecureCloudDb
- ServiceNow ITSM
- Slack
- ThreatModeler
- Vectra AI Cognito Detect

Verfügbarkeit von Standards nach Regionen

Der [AWS Control Tower vom Service verwaltete Standard](#) ist nur in AWS-Regionen den folgenden AWS Control Tower Bereichen verfügbar: AWS GovCloud (US) Regions Eine Liste der Regionen, die AWS Control Tower derzeit unterstützt werden, finden Sie unter [How AWS-Regionen Work With AWS Control Tower](#) im AWS Control Tower Benutzerhandbuch.

Der [AWS Resource Tagging-Standard](#) ist in den folgenden Regionen nicht verfügbar: Asien-Pazifik (Taipeh), Asien-Pazifik (Thailand) und Mexiko (Zentral).

Andere Sicherheitsstandards sind in allen Regionen verfügbar, in denen Security Hub CSPM derzeit verfügbar ist.

Verfügbarkeit von Kontrollen nach Regionen

Einige Security Hub CSPM-Steuerelemente sind nicht in allen Regionen verfügbar. Eine Liste der Steuerelemente, die nicht in jeder Region verfügbar sind, finden Sie unter [Regionale Beschränkungen der Security Hub CSPM-Steuerungen](#)

Auf der Security Hub CSPM-Konsole erscheint ein Steuerelement nicht in der Kontrollliste, wenn es in der Region, in der Sie derzeit angemeldet sind, nicht verfügbar ist. Die Ausnahme ist eine Aggregationsregion. Wenn Sie eine Aggregationsregion festlegen und sich bei dieser Region anmelden, werden in der Konsole Steuerelemente angezeigt, die in der Aggregationsregion oder einer oder mehreren verknüpften Regionen verfügbar sind.

Regionale Beschränkungen der Security Hub CSPM-Steuerungen

Einige AWS Security Hub Cloud Security Posture Management (CSPM) -Steuerelemente sind nicht in allen verfügbar. AWS-Regionen Auf dieser Seite wird angegeben, welche Steuerelemente in bestimmten Regionen nicht verfügbar sind.

Auf der Security Hub CSPM-Konsole erscheint ein Steuerelement nicht in der Kontrollliste, wenn es in der Region, in der Sie derzeit angemeldet sind, nicht verfügbar ist. Die Ausnahme ist eine Aggregationsregion. Wenn Sie eine Aggregationsregion festlegen und sich bei dieser Region anmelden, werden in der Konsole Steuerelemente angezeigt, die in der Aggregationsregion oder einer oder mehreren verknüpften Regionen verfügbar sind.

AWS-Regionen

- [USA Ost \(Nord-Virginia\)](#)
- [USA Ost \(Ohio\)](#)
- [USA West \(Nordkalifornien\)](#)
- [USA West \(Oregon\)](#)
- [Afrika \(Kapstadt\)](#)
- [Asien-Pazifik \(Hongkong\)](#)
- [Asien-Pazifik \(Hyderabad\)](#)
- [Asien-Pazifik \(Jakarta\)](#)
- [Asien-Pazifik \(Malaysia\)](#)
- [Asien-Pazifik \(Melbourne\)](#)
- [Asien-Pazifik \(Mumbai\)](#)
- [Asien-Pazifik \(Osaka\)](#)
- [Asien-Pazifik \(Seoul\)](#)
- [Asien-Pazifik \(Singapur\)](#)
- [Asien-Pazifik \(Sydney\)](#)
- [Asien-Pazifik \(Taipeh\)](#)
- [Asien-Pazifik \(Thailand\)](#)
- [Asien-Pazifik \(Tokio\)](#)
- [Kanada \(Zentral\)](#)

- [Kanada West \(Calgary\)](#)
- [China \(Peking\)](#)
- [China \(Ningxia\)](#)
- [Europa \(Frankfurt\)](#)
- [Europa \(Irland\)](#)
- [Europa \(London\)](#)
- [Europa \(Milan\)](#)
- [Europa \(Paris\)](#)
- [Europa \(Spain\)](#)
- [Europa \(Stockholm\)](#)
- [Europa \(Zürich\)](#)
- [Israel \(Tel Aviv\)](#)
- [Mexiko \(Zentral\)](#)
- [Nahe Osten \(Bahrain\)](#)
- [Nahe Osten \(VAE\)](#)
- [Südamerika \(São Paulo\)](#)
- [AWS GovCloud \(US-Ost\)](#)
- [AWS GovCloud \(US-West\)](#)

USA Ost (Nord-Virginia)

Die folgenden Steuerelemente werden in der Region USA Ost (Nord-Virginia) nicht unterstützt.

- [\[ElastiCache.4\] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden](#)
- [\[ElastiCache.5\] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden](#)
- [\[ElastiCache.6\] Für Replikationsgruppen ElastiCache \(Redis OSS\) früherer Versionen sollte Redis OSS AUTH aktiviert sein](#)
- [\[ElastiCache.7\] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)

USA Ost (Ohio)

Die folgenden Steuerelemente werden in der Region USA Ost (Ohio) nicht unterstützt.

- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[Connect.1\] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden](#)
- [\[Connect.2\] Für Amazon Connect Connect-Instances sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[EC2.24\] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[ECR.4\] Öffentliche ECR-Repositoryn sollten markiert werden](#)

- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[IoT Twin Maker.1\] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden](#)
- [\[IoT Twin Maker.2\] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden](#)
- [\[IoT Twin Maker.3\] AWS TwinMaker IoT-Szenen sollten markiert werden](#)
- [\[IoT Twin Maker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[IoT Wireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[IoT Wireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)
- [\[IoT Wireless .3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)
- [\[RDS.31\] RDS-DB-Sicherheitsgruppen sollten markiert werden](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WorkSpaces.1\] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden](#)
- [\[WorkSpaces.2\] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden](#)

USA West (Nordkalifornien)

Die folgenden Steuerelemente werden in der Region USA West (Nordkalifornien) nicht unterstützt.

- [\[AppRunner.1\] App Runner-Dienste sollten markiert sein](#)
- [\[AppRunner.2\] App Runner VPC-Konnektoren sollten markiert sein](#)

- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[CodeArtifact.1\] CodeArtifact Repositorien sollten mit Tags versehen werden](#)
- [\[CodeGuruProfiler.1\] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden](#)
- [\[CodeGuruReviewer.1\] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden](#)
- [\[Connect.1\] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden](#)
- [\[Connect.2\] Für Amazon Connect Connect-Instances sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[DocumentDB.1\] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DocumentDB.2\] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen](#)
- [\[DocumentDB.3\] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein](#)

- [\[DocumentDB.4\] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch](#)
- [\[DocumentDB.5\] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[DocumentDB.6\] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[ECR.4\] Öffentliche ECR-Repositorien sollten markiert werden](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)
- [\[IoTEvents .1\] AWS IoT-Events-Eingaben sollten markiert werden](#)
- [\[IoTEvents .2\] AWS IoT-Ereignisdetektormodelle sollten markiert werden](#)
- [\[IoTEvents .3\] Alarmmodelle für AWS IoT Events sollten markiert werden](#)
- [\[IoTSiteWise.1\] AWS SiteWise IoT-Asset-Modelle sollten markiert werden](#)
- [\[IoTSiteWise.2\] AWS SiteWise IoT-Dashboards sollten markiert werden](#)
- [\[IoTSiteWise.3\] AWS SiteWise IoT-Gateways sollten markiert werden](#)
- [\[IoTSiteWise.4\] AWS SiteWise IoT-Portale sollten markiert werden](#)
- [\[IoTSiteWise.5\] AWS SiteWise IoT-Projekte sollten markiert werden](#)
- [\[IoT Twin Maker.1\] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden](#)
- [\[IoT Twin Maker.2\] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden](#)
- [\[IoT Twin Maker.3\] AWS TwinMaker IoT-Szenen sollten markiert werden](#)
- [\[IoT Twin Maker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[IoTWireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[IoTWireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)
- [\[IoTWireless .3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)

- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)
- [\[RDS.35\] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein](#)
- [\[Redshift.18\] Für Redshift-Cluster sollten Multi-AZ-Bereitstellungen aktiviert sein](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WorkSpaces.1\] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden](#)
- [\[WorkSpaces.2\] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden](#)

USA West (Oregon)

Die folgenden Steuerelemente werden in der Region USA West (Oregon) nicht unterstützt.

- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)

- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[ECR.4\] Öffentliche ECR-Repositoryn sollten markiert werden](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)

Afrika (Kapstadt)

Die folgenden Steuerelemente werden in der Region Afrika (Kapstadt) nicht unterstützt.

- [\[Amplify.1\] Amplify-Apps sollten markiert werden](#)
- [\[Amplify.2\] Amplify-Zweige sollten markiert werden](#)
- [\[AppRunner.1\] App Runner-Dienste sollten markiert sein](#)
- [\[AppRunner.2\] App Runner VPC-Konnektoren sollten markiert sein](#)
- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)

- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[CodeArtifact.1\] CodeArtifact Repositorien sollten mit Tags versehen werden](#)
- [\[CodeGuruProfiler.1\] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden](#)
- [\[CodeGuruReviewer.1\] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden](#)
- [\[Cognito.1\] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein](#)
- [\[DMS.10\] Bei DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein](#)
- [\[DocumentDB.1\] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DocumentDB.2\] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen](#)
- [\[DocumentDB.3\] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein](#)
- [\[DocumentDB.4\] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch](#)

- [\[DocumentDB.5\] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[DocumentDB.6\] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[DynamoDB.3\] DynamoDB Accelerator \(DAX\) -Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DynamoDB.7\] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[EC2.4\] Gestoppte EC2 Instances sollten nach einem bestimmten Zeitraum entfernt werden](#)
- [\[EC2.8\] EC2 Instances sollten Instance Metadata Service Version 2 \(\) verwenden](#)
- [\[EC2.14\] Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 oder: :/0 auf Port 3389 zulassen](#)
- [\[EC2.24\] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden](#)
- [\[EC2.58\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert sein](#)
- [\[EC2.60\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[EC2.177\] EC2 Traffic Mirror-Sitzungen sollten mit Tags versehen werden](#)
- [\[EC2.179\] EC2 Traffic-Spiegel-Ziele sollten markiert werden](#)
- [\[ECR.4\] Öffentliche ECR-Repositoryn sollten markiert werden](#)
- [\[ELB.2\] Classic Load Balancer mit SSL/HTTPS Listnern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager](#)
- [\[ES.3\] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden](#)
- [\[EventBridge.4\] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[IAM.18\] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde](#) [AWS -Support](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)

- [\[IoT.1\] AWS IoT Device Defender Sicherheitsprofile sollten markiert werden](#)
- [\[IoT.2\] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden](#)
- [\[IoT.3\] AWS IoT Core -Dimensionen sollten markiert werden](#)
- [\[IoT.4\] AWS IoT Core Autorisierer sollten markiert werden](#)
- [\[IoT.5\] AWS IoT Core Rollenalias sollten markiert werden](#)
- [\[IoT.6\] AWS IoT Core Richtlinien sollten markiert werden](#)
- [\[IoT Events .1\] AWS IoT-Events-Eingaben sollten markiert werden](#)
- [\[IoT Events .2\] AWS IoT-Ereignisdetektormodelle sollten markiert werden](#)
- [\[IoT Events .3\] Alarmmodelle für AWS IoT Events sollten markiert werden](#)
- [\[IoT Site Wise.1\] AWS SiteWise IoT-Asset-Modelle sollten markiert werden](#)
- [\[IoT Site Wise.2\] AWS SiteWise IoT-Dashboards sollten markiert werden](#)
- [\[IoT Site Wise.3\] AWS SiteWise IoT-Gateways sollten markiert werden](#)
- [\[IoT Site Wise.4\] AWS SiteWise IoT-Portale sollten markiert werden](#)
- [\[IoT Site Wise.5\] AWS SiteWise IoT-Projekte sollten markiert werden](#)
- [\[IoT TTwin Maker.1\] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden](#)
- [\[IoT TTwin Maker.2\] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden](#)
- [\[IoT TTwin Maker.3\] AWS TwinMaker IoT-Szenen sollten markiert werden](#)
- [\[IoT TTwin Maker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[IoT TWireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[IoT TWireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)
- [\[IoT TWireless .3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)
- [\[Keyspaces.1\] Amazon Keyspaces Keyspaces sollten mit Tags versehen sein](#)
- [\[MSK.3\] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden](#)
- [\[MSK.5\] Bei MSK-Konnektoren sollte die Protokollierung aktiviert sein](#)
- [\[RDS.1\] Der RDS-Snapshot sollte privat sein](#)
- [\[RDS.14\] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein](#)
- [\[RDS.31\] RDS-DB-Sicherheitsgruppen sollten markiert werden](#)

- [\[RedshiftServerless.1\] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden](#)
- [\[RedshiftServerless.2\] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein](#)
- [\[RedshiftServerless.3\] Serverlose Redshift-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten](#)
- [\[RedshiftServerless.4\] Serverlose Redshift-Namespace sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys](#)
- [\[RedshiftServerless.5\] Redshift Serverless-Namespace sollten nicht den Standard-Admin-Benutzernamen verwenden](#)
- [\[RedshiftServerless.6\] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch](#)
- [\[RedshiftServerless.7\] Redshift Serverless-Namespace sollten nicht den Standard-Datenbanknamen verwenden](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)
- [\[SSM.3\] Von Systems Manager verwaltete EC2 Amazon-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)

Asien-Pazifik (Hongkong)

Die folgenden Steuerelemente werden in der Region Asien-Pazifik (Hongkong) nicht unterstützt.

- [\[AppFlow.1\] AppFlow Amazon-Datenflüsse sollten mit Tags versehen werden](#)
- [\[AppRunner.1\] App Runner-Dienste sollten markiert sein](#)
- [\[AppRunner.2\] App Runner VPC-Konnektoren sollten markiert sein](#)

- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[CodeArtifact.1\] CodeArtifact Repositorien sollten mit Tags versehen werden](#)
- [\[CodeGuruProfiler.1\] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden](#)
- [\[CodeGuruReviewer.1\] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden](#)
- [\[Cognito.1\] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein](#)
- [\[Connect.1\] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden](#)
- [\[Connect.2\] Für Amazon Connect Connect-Instances sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[DynamoDB.3\] DynamoDB Accelerator \(DAX\) -Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DynamoDB.7\] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden](#)

- [\[EC2.24\] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden](#)
- [\[EC2.58\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert sein](#)
- [\[EC2.60\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[ECR.4\] Öffentliche ECR-Repositoryn sollten markiert werden](#)
- [\[EventBridge.4\] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)
- [\[IoTEvents.1\] AWS IoT-Events-Eingaben sollten markiert werden](#)
- [\[IoTEvents.2\] AWS IoT-Ereignisdetektormodelle sollten markiert werden](#)
- [\[IoTEvents.3\] Alarmmodelle für AWS IoT Events sollten markiert werden](#)
- [\[IoTSiteWise.1\] AWS SiteWise IoT-Asset-Modelle sollten markiert werden](#)
- [\[IoTSiteWise.2\] AWS SiteWise IoT-Dashboards sollten markiert werden](#)
- [\[IoTSiteWise.3\] AWS SiteWise IoT-Gateways sollten markiert werden](#)
- [\[IoTSiteWise.4\] AWS SiteWise IoT-Portale sollten markiert werden](#)
- [\[IoTSiteWise.5\] AWS SiteWise IoT-Projekte sollten markiert werden](#)
- [\[IoT Twin Maker.1\] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden](#)
- [\[IoT Twin Maker.2\] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden](#)
- [\[IoT Twin Maker.3\] AWS TwinMaker IoT-Szenen sollten markiert werden](#)
- [\[IoT Twin Maker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[IoT Wireless.1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[IoT Wireless.2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)

- [\[IoTWireless .3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)
- [\[MSK.3\] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden](#)
- [\[MSK.5\] Bei MSK-Konnektoren sollte die Protokollierung aktiviert sein](#)
- [\[RDS.14\] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein](#)
- [\[RDS.31\] RDS-DB-Sicherheitsgruppen sollten markiert werden](#)
- [\[RedshiftServerless.1\] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden](#)
- [\[RedshiftServerless.2\] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)
- [\[SES.1\] SES-Kontaktlisten sollten mit Tags versehen werden](#)
- [\[SES.2\] SES-Konfigurationssätze sollten mit Tags versehen werden](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WorkSpaces.1\] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden](#)
- [\[WorkSpaces.2\] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden](#)

Asien-Pazifik (Hyderabad)

Die folgenden Steuerelemente werden in der Region Asien-Pazifik (Hyderabad) nicht unterstützt.

- [\[Account.2\] AWS-Konten sollte Teil einer Organisation sein AWS Organizations](#)

- [\[APIGateway.8\] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben](#)
- [\[APIGateway.9\] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein](#)
- [\[Amplify.1\] Amplify-Apps sollten markiert werden](#)
- [\[Amplify.2\] Amplify-Zweige sollten markiert werden](#)
- [\[AppConfig.1\] AWS AppConfig Anwendungen sollten markiert werden](#)
- [\[AppConfig.2\] AWS AppConfig Konfigurationsprofile sollten mit Tags versehen werden](#)
- [\[AppConfig.3\] AWS AppConfig Umgebungen sollten markiert werden](#)
- [\[AppFlow.1\] AppFlow Amazon-Datenflüsse sollten mit Tags versehen werden](#)
- [\[AppRunner.1\] App Runner-Dienste sollten markiert sein](#)
- [\[AppRunner.2\] App Runner VPC-Konnektoren sollten markiert sein](#)
- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [\[Backup.1\] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein](#)
- [\[Backup.4\] AWS Backup Berichtspläne sollten markiert werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)

- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[CloudTrail.6\] Sicherstellen, dass der S3-Bucket, in dem CloudTrail Protokolle gespeichert werden, nicht öffentlich zugänglich ist](#)
- [\[CloudTrail.7\] Sicherstellen, dass die S3-Bucket-Zugriffsprotokollierung für den CloudTrail S3-Bucket aktiviert ist](#)
- [\[CodeArtifact.1\] CodeArtifact Repositorien sollten mit Tags versehen werden](#)
- [\[CodeGuruProfiler.1\] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden](#)
- [\[CodeGuruReviewer.1\] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden](#)
- [\[Cognito.1\] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein](#)
- [\[Cognito.2\] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen](#)
- [\[Connect.1\] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden](#)
- [\[Connect.2\] Für Amazon Connect Connect-Instances sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[Detective.1\] Verhaltensdiagramme von Detektiven sollten markiert werden](#)
- [\[DMS.2\] DMS-Zertifikate sollten gekennzeichnet sein](#)
- [\[DMS.3\] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden](#)
- [\[DMS.4\] DMS-Replikationsinstanzen sollten markiert werden](#)
- [\[DMS.5\] Subnetzgruppen für die DMS-Replikation sollten markiert werden](#)
- [\[DMS.6\] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein](#)
- [\[DMS.7\] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.8\] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.9\] DMS-Endpunkte sollten SSL verwenden](#)
- [\[DMS.10\] Bei DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein](#)
- [\[DMS.11\] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein](#)
- [\[DMS.12\] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein](#)

- [\[DynamoDB.3\] DynamoDB Accelerator \(DAX\) -Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DynamoDB.4\] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein](#)
- [\[DynamoDB.7\] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[EC2.14\] Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 oder: :/0 auf Port 3389 zulassen](#)
- [\[EC2.22\] Ungenutzte EC2 Amazon-Sicherheitsgruppen sollten entfernt werden](#)
- [\[EC2.24\] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden](#)
- [\[EC2.25\] EC2 Amazon-Startvorlagen sollten Netzwerkschnittstellen nicht öffentlich IPs zuweisen](#)
- [\[EC2.28\] EBS-Volumes sollten durch einen Backup-Plan abgedeckt sein](#)
- [\[EC2.34\] Die Routentabellen für EC2 Transit-Gateways sollten mit Tags versehen werden](#)
- [\[EC2.40\] EC2 NAT-Gateways sollten markiert werden](#)
- [\[EC2.48\] Amazon VPC-Flow-Logs sollten mit Tags versehen werden](#)
- [\[EC2.51\] EC2 Client-VPN-Endpunkte sollten die Client-Verbindungsprotokollierung aktiviert haben](#)
- [\[EC2.58\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert sein](#)
- [\[EC2.60\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden](#)
- [\[EC2.170\] EC2 Startvorlagen sollten Instance Metadata Service Version 2 \(\) verwenden IMDSv2](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[EC2.175\] EC2 Startvorlagen sollten mit Tags versehen sein](#)
- [\[EC2.177\] EC2 Traffic Mirror-Sitzungen sollten mit Tags versehen werden](#)
- [\[EC2.179\] EC2 Traffic-Spiegel-Ziele sollten markiert werden](#)
- [\[EC2.180\] Bei EC2 Netzwerkschnittstellen sollte die source/destination Überprüfung aktiviert sein](#)
- [\[ECR.4\] Öffentliche ECR-Repositoryn sollten markiert werden](#)
- [\[EFS.1\] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS](#)
- [\[EFS.2\] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein](#)
- [\[ELB.14\] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden](#)
- [\[ELB.17\] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden](#)

- [\[ELB.18\] Anwendungs- und Network Load Balancer Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln](#)
- [Bei \[ElastiCache.1\] ElastiCache \(Redis OSS\) -Clustern sollten automatische Backups aktiviert sein](#)
- [\[ElastiCache.6\] Für Replikationsgruppen ElastiCache \(Redis OSS\) früherer Versionen sollte Redis OSS AUTH aktiviert sein](#)
- [\[ElastiCache.7\] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden](#)
- [\[ElasticBeanstalk.1\] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben](#)
- [\[ElasticBeanstalk.2\] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk sollte Logs streamen nach CloudWatch](#)
- [\[EMR.1\] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben](#)
- [\[ES.4\] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein](#)
- [\[EventBridge.4\] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[Glue.4\] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue](#)
- [\[GuardDuty.2\] GuardDuty Filter sollten mit Tags versehen sein](#)
- [\[IAM.1\] IAM-Richtlinien sollten keine vollen „*“-Administratorrechte zulassen](#)
- [\[IAM.2\] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein](#)
- [\[IAM.3\] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden](#)
- [\[IAM.5\] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen](#)
- [\[IAM.8\] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden](#)
- [\[IAM.18\] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS -Support](#)
- [\[IAM.19\] MFA sollte für alle IAM-Benutzer aktiviert sein](#)
- [\[IAM.21\] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen](#)

- [\[IAM.22\] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden](#)
- [\[IAM.24\] IAM-Rollen sollten mit Tags versehen werden](#)
- [\[IAM.25\] IAM-Benutzer sollten markiert werden](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[IAM.27\] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWS Cloud Shell Full Access](#)
- [\[Inspector.1\] Das EC2 Scannen mit Amazon Inspector sollte aktiviert sein](#)
- [\[Inspector.2\] Das Amazon Inspector ECR-Scannen sollte aktiviert sein](#)
- [\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)
- [\[Inspector.4\] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein](#)
- [\[IoT.1\] AWS IoT Device Defender Sicherheitsprofile sollten markiert werden](#)
- [\[IoT.2\] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden](#)
- [\[IoT.3\] AWS IoT Core -Dimensionen sollten markiert werden](#)
- [\[IoT.4\] AWS IoT Core Autorisierer sollten markiert werden](#)
- [\[IoT.5\] AWS IoT Core Rollenalias sollten markiert werden](#)
- [\[IoT.6\] AWS IoT Core Richtlinien sollten markiert werden](#)
- [\[IoT Events .1\] AWS IoT-Events-Eingaben sollten markiert werden](#)
- [\[IoT Events .2\] AWS IoT-Ereignisdetektormodelle sollten markiert werden](#)
- [\[IoT Events .3\] Alarmmodelle für AWS IoT Events sollten markiert werden](#)
- [\[IoT Site Wise.1\] AWS SiteWise IoT-Asset-Modelle sollten markiert werden](#)
- [\[IoT Site Wise.2\] AWS SiteWise IoT-Dashboards sollten markiert werden](#)
- [\[IoT Site Wise.3\] AWS SiteWise IoT-Gateways sollten markiert werden](#)
- [\[IoT Site Wise.4\] AWS SiteWise IoT-Portale sollten markiert werden](#)
- [\[IoT Site Wise.5\] AWS SiteWise IoT-Projekte sollten markiert werden](#)
- [\[IoT Twin Maker.1\] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden](#)
- [\[IoT Twin Maker.2\] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden](#)
- [\[IoT Twin Maker.3\] AWS TwinMaker IoT-Szenen sollten markiert werden](#)
- [\[IoT Twin Maker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[IoT Wireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[IoT Wireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)

- [\[IoTWireless.3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)
- [\[Keyspaces.1\] Amazon Keyspaces Keyspaces sollten mit Tags versehen sein](#)
- [\[KMS.1\] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)
- [\[KMS.2\] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)
- [\[Lambda.7\] Bei Lambda-Funktionen sollte aktives Tracing aktiviert sein AWS X-Ray](#)
- [\[Macie.1\] Amazon Macie sollte aktiviert sein](#)
- [\[Macie.2\] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein](#)
- [\[MQ.2\] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch](#)
- [\[MQ.3\] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein](#)
- [\[MQ.4\] Amazon MQ-Broker sollten markiert werden](#)
- [\[MQ.5\] ActiveMQ-Broker sollten den Aktiv-/Standby-Bereitstellungsmodus verwenden](#)
- [\[MQ.6\] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden](#)
- [\[MSK.3\] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden](#)
- [\[MSK.4\] Bei MSK-Clustern sollte der öffentliche Zugriff deaktiviert sein](#)
- [\[MSK.5\] Bei MSK-Konnektoren sollte die Protokollierung aktiviert sein](#)
- [\[MSK.6\] MSK-Cluster sollten den nicht authentifizierten Zugriff deaktivieren](#)
- [\[Neptune.1\] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.2\] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)
- [\[Neptune.3\] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein](#)
- [\[Neptune.4\] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[Neptune.5\] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein](#)
- [\[Neptune.6\] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.7\] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein](#)
- [\[Neptune.8\] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren](#)
- [\[Neptune.9\] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden](#)

- [Bei \[Opensearch.1\] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein](#)
- [\[Opensearch.2\] OpenSearch -Domains sollten nicht öffentlich zugänglich sein](#)
- [\[Opensearch.3\] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden](#)
- [Die Protokollierung von \[Opensearch.4\] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein](#)
- [Für \[Opensearch.5\] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein](#)
- [\[Opensearch.6\] OpenSearch Domains sollten mindestens drei Datenknoten haben](#)
- [Für \[Opensearch.7\] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein](#)
- [\[Opensearch.8\] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden](#)
- [\[Opensearch.9\] OpenSearch -Domains sollten mit Tags versehen werden](#)
- [Auf \[Opensearch.10\] OpenSearch -Domains sollte das neueste Softwareupdate installiert sein](#)
- [\[Opensearch.11\] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben](#)
- [\[RDS.14\] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein](#)
- [\[RDS.15\] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden](#)
- [\[RDS.26\] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden](#)
- [\[RDS.31\] RDS-DB-Sicherheitsgruppen sollten markiert werden](#)
- [\[RDS.35\] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein](#)
- [\[RDS.37\] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[Redshift.10\] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[Redshift.18\] Für Redshift-Cluster sollten Multi-AZ-Bereitstellungen aktiviert sein](#)
- [\[RedshiftServerless.1\] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden](#)
- [\[RedshiftServerless.2\] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein](#)
- [\[RedshiftServerless.3\] Serverlose Redshift-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten](#)
- [\[RedshiftServerless.4\] Serverlose Redshift-Namespaces sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys](#)
- [\[RedshiftServerless.5\] Redshift Serverless-Namespaces sollten nicht den Standard-Admin-Benutzernamen verwenden](#)

- [\[RedshiftServerless.6\] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch](#)
- [\[RedshiftServerless.7\] Redshift Serverless-Namespaces sollten nicht den Standard-Datenbanknamen verwenden](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.6\] Allgemeine S3-Bucket-Richtlinien sollten den Zugriff auf andere einschränken AWS-Konten](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)
- [\[SageMaker.1\] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben](#)
- [\[SageMaker.2\] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden](#)
- [\[SageMaker.3\] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben](#)
- [\[SageMaker.5\] SageMaker Modelle sollten eingehenden Datenverkehr blockieren](#)
- [\[SageMaker.6\] SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden](#)
- [\[SageMaker.7\] SageMaker Bilder sollten mit Tags versehen werden](#)
- [\[SES.1\] SES-Kontaktlisten sollten mit Tags versehen werden](#)
- [\[SES.2\] SES-Konfigurationssätze sollten mit Tags versehen werden](#)
- [\[SQS.1\] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt werden](#)
- [\[SQS.2\] SQS-Warteschlangen sollten markiert werden](#)
- [\[SQS.3\] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen](#)
- [\[SSM.3\] Von Systems Manager verwaltete EC2 Amazon-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben](#)
- [\[SSM.6\] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[SSM.7\] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein](#)
- [\[Transfer.3\] Bei Connectoren der Transfer-Familie sollte die Protokollierung aktiviert sein](#)
- [\[Transfer.4\] Transfer Family Familienverträge sollten gekennzeichnet werden](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.3\] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben](#)

- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WAF.10\] AWS WAF web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WAF.11\] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WorkSpaces.1\] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden](#)
- [\[WorkSpaces.2\] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden](#)

Asien-Pazifik (Jakarta)

Die folgenden Steuerelemente werden in der Region Asien-Pazifik (Jakarta) nicht unterstützt.

- [\[Account.2\] AWS-Konten sollte Teil einer Organisation sein AWS Organizations](#)
- [\[APIGateway.8\] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben](#)
- [\[APIGateway.9\] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein](#)
- [\[Amplify.1\] Amplify-Apps sollten markiert werden](#)
- [\[Amplify.2\] Amplify-Zweige sollten markiert werden](#)
- [\[AppFlow.1\] AppFlow Amazon-Datenflüsse sollten mit Tags versehen werden](#)
- [\[AppRunner.1\] App Runner-Dienste sollten markiert sein](#)
- [\[AppRunner.2\] App Runner VPC-Konnektoren sollten markiert sein](#)
- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [\[Backup.1\] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein](#)
- [\[Backup.4\] AWS Backup Berichtspläne sollten markiert werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)

- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[CodeArtifact.1\] CodeArtifact Repositorien sollten mit Tags versehen werden](#)
- [\[CodeBuild.1\] Das CodeBuild Bitbucket-Quell-Repository URLs sollte keine vertraulichen Anmeldeinformationen enthalten](#)
- [\[CodeBuild.2\] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten](#)
- [\[CodeBuild.3\] CodeBuild S3-Protokolle sollten verschlüsselt sein](#)
- [\[CodeBuild.4\] CodeBuild Projektumgebungen sollten eine AWS Config Protokollierungsdauer haben](#)
- [\[CodeGuruProfiler.1\] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden](#)
- [\[CodeGuruReviewer.1\] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden](#)
- [\[Cognito.1\] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein](#)
- [\[Connect.1\] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden](#)
- [\[Connect.2\] Für Amazon Connect Connect-Instances sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[Detective.1\] Verhaltensdiagramme von Detektiven sollten markiert werden](#)
- [\[DMS.2\] DMS-Zertifikate sollten gekennzeichnet sein](#)
- [\[DMS.3\] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden](#)
- [\[DMS.4\] DMS-Replikationsinstanzen sollten markiert werden](#)
- [\[DMS.5\] Subnetzgruppen für die DMS-Replikation sollten markiert werden](#)

- [\[DMS.6\] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein](#)
- [\[DMS.7\] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.8\] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.9\] DMS-Endpunkte sollten SSL verwenden](#)
- [\[DMS.10\] Bei DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein](#)
- [\[DMS.11\] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein](#)
- [\[DMS.12\] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein](#)
- [\[DocumentDB.1\] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DocumentDB.2\] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen](#)
- [\[DocumentDB.3\] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein](#)
- [\[DocumentDB.4\] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch](#)
- [\[DocumentDB.5\] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[DocumentDB.6\] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[DynamoDB.3\] DynamoDB Accelerator \(DAX\) -Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DynamoDB.4\] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein](#)
- [\[DynamoDB.7\] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[EC2.14\] Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 oder: :/0 auf Port 3389 zulassen](#)
- [\[EC2.22\] Ungenutzte EC2 Amazon-Sicherheitsgruppen sollten entfernt werden](#)
- [\[EC2.24\] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden](#)
- [\[EC2.28\] EBS-Volumes sollten durch einen Backup-Plan abgedeckt sein](#)
- [\[EC2.51\] EC2 Client-VPN-Endpunkte sollten die Client-Verbindungsprotokollierung aktiviert haben](#)
- [\[EC2.58\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert sein](#)

- [\[EC2.60\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[EC2.177\] EC2 Traffic Mirror-Sitzungen sollten mit Tags versehen werden](#)
- [\[EC2.179\] EC2 Traffic-Spiegel-Ziele sollten markiert werden](#)
- [\[ECR.4\] Öffentliche ECR-Repositoryn sollten markiert werden](#)
- [\[EFS.1\] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS](#)
- [\[EFS.2\] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein](#)
- [\[ELB.17\] Anwendungs- und Netzwerk-Load-Balancer mit Listnern sollten die empfohlenen Sicherheitsrichtlinien verwenden](#)
- [\[ELB.18\] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln](#)
- [Bei \[ElastiCache.1\] ElastiCache \(Redis OSS\) -Clustern sollten automatische Backups aktiviert sein](#)
- [\[ElastiCache.6\] Für Replikationsgruppen ElastiCache \(Redis OSS\) früherer Versionen sollte Redis OSS AUTH aktiviert sein](#)
- [\[ElastiCache.7\] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden](#)
- [\[ElasticBeanstalk.1\] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben](#)
- [\[ElasticBeanstalk.2\] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein](#)
- [\[EventBridge.4\] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[GuardDuty.2\] GuardDuty Filter sollten mit Tags versehen sein](#)
- [\[IAM.18\] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS -Support](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)

- [\[IoT.1\] AWS IoT Device Defender Sicherheitsprofile sollten markiert werden](#)
- [\[IoT.2\] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden](#)
- [\[IoT.3\] AWS IoT Core -Dimensionen sollten markiert werden](#)
- [\[IoT.4\] AWS IoT Core Autorisierer sollten markiert werden](#)
- [\[IoT.5\] AWS IoT Core Rollenalias sollten markiert werden](#)
- [\[IoT.6\] AWS IoT Core Richtlinien sollten markiert werden](#)
- [\[IoT Events .1\] AWS IoT-Events-Eingaben sollten markiert werden](#)
- [\[IoT Events .2\] AWS IoT-Ereignisdetektormodelle sollten markiert werden](#)
- [\[IoT Events .3\] Alarmmodelle für AWS IoT Events sollten markiert werden](#)
- [\[IoT Site Wise.1\] AWS SiteWise IoT-Asset-Modelle sollten markiert werden](#)
- [\[IoT Site Wise.2\] AWS SiteWise IoT-Dashboards sollten markiert werden](#)
- [\[IoT Site Wise.3\] AWS SiteWise IoT-Gateways sollten markiert werden](#)
- [\[IoT Site Wise.4\] AWS SiteWise IoT-Portale sollten markiert werden](#)
- [\[IoT Site Wise.5\] AWS SiteWise IoT-Projekte sollten markiert werden](#)
- [\[IoT TTwin Maker.1\] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden](#)
- [\[IoT TTwin Maker.2\] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden](#)
- [\[IoT TTwin Maker.3\] AWS TwinMaker IoT-Szenen sollten markiert werden](#)
- [\[IoT TTwin Maker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[IoT TWireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[IoT TWireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)
- [\[IoT TWireless .3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)
- [\[Keyspaces.1\] Amazon Keyspaces Keyspaces sollten mit Tags versehen sein](#)
- [\[Macie.1\] Amazon Macie sollte aktiviert sein](#)
- [\[Macie.2\] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein](#)
- [\[MSK.3\] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden](#)
- [\[MSK.5\] Bei MSK-Konnektoren sollte die Protokollierung aktiviert sein](#)
- [\[Neptune.1\] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden](#)

- [\[Neptune.2\] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)
- [\[Neptune.3\] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein](#)
- [\[Neptune.4\] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[Neptune.5\] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein](#)
- [\[Neptune.6\] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.7\] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein](#)
- [\[Neptune.8\] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren](#)
- [\[Neptune.9\] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden](#)
- [Für \[Opensearch.5\] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein](#)
- [\[Opensearch.6\] OpenSearch Domains sollten mindestens drei Datenknoten haben](#)
- [\[RDS.14\] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein](#)
- [\[RDS.26\] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden](#)
- [\[RDS.31\] RDS-DB-Sicherheitsgruppen sollten markiert werden](#)
- [\[RedshiftServerless.1\] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden](#)
- [\[RedshiftServerless.2\] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.11\] Bei S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)
- [\[ServiceCatalog.1\] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden](#)
- [\[SQS.1\] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt werden](#)
- [\[SQS.2\] SQS-Warteschlangen sollten markiert werden](#)
- [\[SQS.3\] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen](#)
- [\[SSM.3\] Von Systems Manager verwaltete EC2 Amazon-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben](#)

- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.3\] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WAF.10\] AWS WAF web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WorkSpaces.1\] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden](#)
- [\[WorkSpaces.2\] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden](#)

Asien-Pazifik (Malaysia)

Die folgenden Steuerelemente werden in der Region Asien-Pazifik (Malaysia) nicht unterstützt.

- [\[ACM.1\] Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden](#)
- [\[ACM.2\] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden](#)
- [\[Account.1\] Sicherheitskontakthinformationen sollten bereitgestellt werden für AWS-Konto](#)
- [\[Account.2\] AWS-Konten sollte Teil einer Organisation sein AWS Organizations](#)
- [\[APIGateway.8\] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben](#)
- [\[APIGateway.9\] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein](#)
- [\[Amplify.1\] Amplify-Apps sollten markiert werden](#)
- [\[Amplify.2\] Amplify-Zweige sollten markiert werden](#)
- [\[AppConfig.1\] AWS AppConfig Anwendungen sollten markiert werden](#)
- [\[AppConfig.2\] AWS AppConfig Konfigurationsprofile sollten mit Tags versehen werden](#)
- [\[AppConfig.3\] AWS AppConfig Umgebungen sollten markiert werden](#)
- [\[AppConfig.4\] AWS AppConfig Erweiterungszuordnungen sollten markiert werden](#)
- [\[AppFlow.1\] AppFlow Amazon-Datenflüsse sollten mit Tags versehen werden](#)
- [\[AppRunner.1\] App Runner-Dienste sollten markiert sein](#)
- [\[AppRunner.2\] App Runner VPC-Konnektoren sollten markiert sein](#)
- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)

- [\[AppSync.2\] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben](#)
- [\[AppSync.4\] AWS AppSync GraphQL APIs sollte markiert sein](#)
- [\[AppSync.5\] AWS AppSync GraphQL APIs sollte nicht mit API-Schlüsseln authentifiziert werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [\[Athena.2\] Athena-Datenkataloge sollten mit Tags versehen werden](#)
- [\[Athena.3\] Athena-Arbeitsgruppen sollten markiert werden](#)
- [\[Athena.4\] Bei Athena-Arbeitsgruppen sollte die Protokollierung aktiviert sein](#)
- [\[AutoScaling.2\] Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken](#)
- [\[AutoScaling.3\] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2 Instances so konfigurieren, dass sie Instance Metadata Service Version 2 \(IMDSv2\) benötigen](#)
- [\[AutoScaling.6\] Auto Scaling Scaling-Gruppen sollten mehrere Instance-Typen in mehreren Availability Zones verwenden](#)
- [\[AutoScaling.9\] Amazon EC2 Auto Scaling Scaling-Gruppen sollten EC2 Amazon-Startvorlagen verwenden](#)
- [\[Backup.1\] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein](#)
- [\[Backup.2\] AWS Backup Wiederherstellungspunkte sollten markiert werden](#)
- [\[Backup.3\] AWS Backup Tresore sollten markiert sein](#)
- [\[Backup.4\] AWS Backup Berichtspläne sollten markiert werden](#)
- [\[Backup.5\] AWS Backup Backup-Pläne sollten markiert werden](#)
- [\[Batch.1\] Warteschlangen für Batch-Jobs sollten markiert werden](#)
- [\[Batch.2\] Richtlinien für die Batch-Planung sollten gekennzeichnet sein](#)
- [\[Batch.3\] Batch-Computing-Umgebungen sollten markiert werden](#)
- [\[Batch.4\] Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden](#)
- [\[CloudFormation.2\] CloudFormation Stapel sollten markiert werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)

- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[CloudTrail.6\] Sicherstellen, dass der S3-Bucket, in dem CloudTrail Protokolle gespeichert werden, nicht öffentlich zugänglich ist](#)
- [\[CloudTrail.7\] Sicherstellen, dass die S3-Bucket-Zugriffsprotokollierung für den CloudTrail S3-Bucket aktiviert ist](#)
- [\[CloudTrail.10\] Event-Datenspeicher in CloudTrail Lake sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys](#)
- [\[CloudWatch.17\] CloudWatch Alarmaktionen sollten aktiviert sein](#)
- [\[CodeArtifact.1\] CodeArtifact Repositorien sollten mit Tags versehen werden](#)
- [\[CodeBuild.1\] Das CodeBuild Bitbucket-Quell-Repository URLs sollte keine vertraulichen Anmeldeinformationen enthalten](#)
- [\[CodeBuild.2\] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten](#)
- [\[CodeBuild.3\] CodeBuild S3-Protokolle sollten verschlüsselt sein](#)
- [\[CodeBuild.4\] CodeBuild Projektumgebungen sollten eine AWS Config Protokollierungsdauer haben](#)
- [\[CodeBuild.7\] Exporte von CodeBuild Berichtsgruppen sollten im Ruhezustand verschlüsselt werden](#)
- [\[CodeGuruProfiler.1\] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden](#)

- [\[CodeGuruReviewer.1\] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden](#)
- [\[Cognito.1\] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein](#)
- [\[Cognito.2\] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen](#)
- [\[Connect.1\] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden](#)
- [\[Connect.2\] Für Amazon Connect Connect-Instances sollte die Protokollierung aktiviert sein](#)
[CloudWatch](#)
- [\[DataFirehose.1\] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden](#)
- [\[DataSync.1\] Für DataSync Aufgaben sollte die Protokollierung aktiviert sein](#)
- [\[DataSync.2\] DataSync Aufgaben sollten mit Tags versehen werden](#)
- [\[Detective.1\] Verhaltensdiagramme von Detektiven sollten markiert werden](#)
- [\[DMS.2\] DMS-Zertifikate sollten gekennzeichnet sein](#)
- [\[DMS.3\] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden](#)
- [\[DMS.4\] DMS-Replikationsinstanzen sollten markiert werden](#)
- [\[DMS.5\] Subnetzgruppen für die DMS-Replikation sollten markiert werden](#)
- [\[DMS.6\] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein](#)
- [\[DMS.7\] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.8\] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.9\] DMS-Endpunkte sollten SSL verwenden](#)
- [\[DMS.10\] Bei DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein](#)
- [\[DMS.11\] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein](#)
- [\[DMS.12\] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein](#)
- [\[DocumentDB.1\] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DocumentDB.2\] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen](#)
- [\[DocumentDB.3\] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein](#)

- [\[DocumentDB.4\] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch](#)
- [\[DocumentDB.5\] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[DocumentDB.6\] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[DynamoDB.3\] DynamoDB Accelerator \(DAX\) -Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DynamoDB.4\] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein](#)
- [\[DynamoDB.6\] Bei DynamoDB-Tabellen sollte der Löschschutz aktiviert sein](#)
- [\[DynamoDB.7\] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[EC2.4\] Gestoppte EC2 Instances sollten nach einem bestimmten Zeitraum entfernt werden](#)
- [\[EC2.21\] Das Netzwerk ACLs sollte keinen Zugang von 0.0.0.0/0 zu Port 22 oder Port 3389 zulassen](#)
- [\[EC2.22\] Ungenutzte EC2 Amazon-Sicherheitsgruppen sollten entfernt werden](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways sollte VPC-Anhangsanfragen nicht automatisch akzeptieren](#)
- [\[EC2.24\] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden](#)
- [\[EC2.25\] EC2 Amazon-Startvorlagen sollten Netzwerkschnittstellen nicht öffentlich IPs zuweisen](#)
- [\[EC2.28\] EBS-Volumes sollten durch einen Backup-Plan abgedeckt sein](#)
- [\[EC2.33\] EC2 Transit-Gateway-Anhänge sollten mit Tags versehen werden](#)
- [\[EC2.34\] Die Routentabellen für EC2 Transit-Gateways sollten mit Tags versehen werden](#)
- [\[EC2.40\] EC2 NAT-Gateways sollten markiert werden](#)
- [\[EC2.48\] Amazon VPC-Flow-Logs sollten mit Tags versehen werden](#)
- [\[EC2.51\] EC2 Client-VPN-Endpunkte sollten die Client-Verbindungsprotokollierung aktiviert haben](#)
- [\[EC2.52\] EC2 Transit-Gateways sollten markiert werden](#)
- [\[EC2.53\] EC2 Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 zu Remote-Serververwaltungsports zulassen](#)
- [\[EC2.54\] EC2 Sicherheitsgruppen sollten keinen Zugriff von: :/0 zu Remote-Serveradministrationsports zulassen](#)
- [\[EC2.55\] VPCs sollte mit einem Schnittstellenendpunkt für die ECR-API konfiguriert werden](#)
- [\[EC2.56\] VPCs sollte mit einem Schnittstellenendpunkt für Docker Registry konfiguriert werden](#)
- [\[EC2.57\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager konfiguriert werden](#)

- [\[EC2.58\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert sein](#)
- [\[EC2.60\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden](#)
- [\[EC2.170\] EC2 Startvorlagen sollten Instance Metadata Service Version 2 \(\) verwenden IMDSv2](#)
- [\[EC2.171\] Bei EC2 VPN-Verbindungen sollte die Protokollierung aktiviert sein](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[EC2.174\] EC2 DHCP-Optionssätze sollten mit Tags versehen werden](#)
- [\[EC2.175\] EC2 Startvorlagen sollten mit Tags versehen sein](#)
- [\[EC2.176\] EC2 Präfixlisten sollten mit Tags versehen werden](#)
- [\[EC2.177\] EC2 Traffic Mirror-Sitzungen sollten mit Tags versehen werden](#)
- [\[EC2.178\] Filter für EC2 Verkehrsspiegel sollten mit Tags versehen werden](#)
- [\[EC2.179\] EC2 Traffic-Spiegel-Ziele sollten markiert werden](#)
- [\[EC2.180\] Bei EC2 Netzwerkschnittstellen sollte die source/destination Überprüfung aktiviert sein](#)
- [\[ECR.1\] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein](#)
- [\[ECR.2\] Bei privaten ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein](#)
- [\[ECR.3\] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein](#)
- [\[ECR.4\] Öffentliche ECR-Repositoryn sollten markiert werden](#)
- [\[ECR.5\] ECR-Repositorys sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys](#)
- [\[ECS.3\] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen](#)
- [\[ECS.4\] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden](#)
- [\[ECS.5\] ECS-Container sollten auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sein](#)
- [\[ECS.8\] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden](#)
- [\[ECS.9\] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen](#)
- [\[ECS.10\] Die ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen](#)
- [\[ECS.12\] ECS-Cluster sollten Container Insights verwenden](#)
- [\[ECS.16\] ECS-Aufgabensätze sollten öffentliche IP-Adressen nicht automatisch zuweisen](#)
- [\[ECS.17\] ECS-Aufgabendefinitionen sollten nicht den Host-Netzwerkmodus verwenden](#)

- [\[EFS.1\] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS](#)
- [\[EFS.2\] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein](#)
- [\[EFS.3\] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen](#)
- [\[EFS.4\] EFS-Zugangspunkte sollten eine Benutzeridentität erzwingen](#)
- [\[EFS.5\] EFS-Zugangspunkte sollten markiert werden](#)
- [\[EFS.6\] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden](#)
- [\[EFS.7\] Bei EFS-Dateisystemen sollten automatische Backups aktiviert sein](#)
- [\[EFS.8\] EFS-Dateisysteme sollten im Ruhezustand verschlüsselt werden](#)
- [\[EKS.2\] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden](#)
- [\[EKS.3\] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden](#)
- [\[EKS.6\] EKS-Cluster sollten markiert werden](#)
- [\[EKS.7\] Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden](#)
- [\[EKS.8\] Bei EKS-Clustern sollte die Auditprotokollierung aktiviert sein](#)
- [\[ELB.10\] Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken](#)
- [\[ELB.12\] Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden](#)
- [\[ELB.13\] Anwendungs-, Netzwerk- und Gateway-Load Balancer sollten sich über mehrere Availability Zones erstrecken](#)
- [\[ELB.14\] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden](#)
- [\[ELB.17\] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden](#)
- [\[ELB.18\] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln](#)
- [Bei \[ElastiCache.1\] ElastiCache \(Redis OSS\) -Clustern sollten automatische Backups aktiviert sein](#)
- [\[ElastiCache.2\] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein](#)
- [\[ElastiCache.3\] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein](#)
- [\[ElastiCache.4\] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden](#)
- [\[ElastiCache.5\] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden](#)

- [\[ElastiCache.6\] Für Replikationsgruppen ElastiCache \(Redis OSS\) früherer Versionen sollte Redis OSS AUTH aktiviert sein](#)
- [\[ElastiCache.7\] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden](#)
- [\[ElasticBeanstalk.1\] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben](#)
- [\[ElasticBeanstalk.2\] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk sollte Logs streamen nach CloudWatch](#)
- [\[EMR.1\] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben](#)
- [\[EMR.2\] Die Amazon EMR-Einstellung zum Blockieren des öffentlichen Zugriffs sollte aktiviert sein](#)
- [\[EMR.3\] Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden](#)
- [\[EMR.4\] Amazon EMR-Sicherheitskonfigurationen sollten bei der Übertragung verschlüsselt werden](#)
- [\[ES.4\] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein](#)
- [\[ES.9\] Elasticsearch-Domains sollten markiert werden](#)
- [\[EventBridge.2\] EventBridge Eventbusse sollten gekennzeichnet sein](#)
- [\[EventBridge.3\] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden](#)
- [\[EventBridge.4\] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[FSx.1\] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden](#)
- [\[FSx.2\] FSx für Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden](#)
- [\[FSx.3\] FSx für OpenZFS-Dateisysteme sollte für die Multi-AZ-Bereitstellung konfiguriert werden](#)
- [\[FSx.4\] FSx für NetApp ONTAP-Dateisysteme sollte für die Multi-AZ-Bereitstellung konfiguriert sein](#)
- [\[FSx.5\] FSx für Windows-Dateiserver sollten für die Multi-AZ-Bereitstellung konfiguriert sein](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[Glue.1\] AWS Glue Jobs sollten markiert werden](#)

- [\[Glue.3\] Transformationen für AWS Glue maschinelles Lernen sollten im Ruhezustand verschlüsselt werden](#)
- [\[Glue.4\] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue](#)
- [\[GuardDuty.2\] GuardDuty Filter sollten mit Tags versehen sein](#)
- [\[GuardDuty.3\] GuardDuty IPSets sollte markiert werden](#)
- [\[GuardDuty.4\] GuardDuty Detektoren sollten markiert werden](#)
- [\[GuardDuty.5\] GuardDuty EKS Audit Log Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.6\] GuardDuty Lambda Protection sollte aktiviert sein](#)
- [\[GuardDuty.7\] GuardDuty EKS Runtime Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.8\] Der GuardDuty Malware-Schutz für EC2 sollte aktiviert sein](#)
- [\[GuardDuty.9\] Der GuardDuty RDS-Schutz sollte aktiviert sein](#)
- [\[GuardDuty.10\] Der GuardDuty S3-Schutz sollte aktiviert sein](#)
- [\[GuardDuty.11\] GuardDuty Runtime Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.12\] GuardDuty ECS Runtime Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.13\] GuardDuty EC2 Runtime Monitoring sollte aktiviert sein](#)
- [\[IAM.1\] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen](#)
- [\[IAM.2\] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein](#)
- [\[IAM.3\] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden](#)
- [\[IAM.4\] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren](#)
- [\[IAM.5\] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen](#)
- [\[IAM.6\] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.](#)
- [\[IAM.7\] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein](#)
- [\[IAM.8\] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden](#)
- [\[IAM.9\] MFA sollte für den Root-Benutzer aktiviert sein](#)
- [\[IAM.10\] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein](#)
- [\[IAM.11\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert](#)
- [\[IAM.12\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert](#)

- [\[IAM.13\] Stellen Sie sicher, dass für die IAM-Passwortrichtlinie mindestens ein Symbol erforderlich ist](#)
- [\[IAM.14\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert](#)
- [\[IAM.15\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert](#)
- [\[IAM.16\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert](#)
- [\[IAM.17\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft](#)
- [\[IAM.18\] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS -Support](#)
- [\[IAM.19\] MFA sollte für alle IAM-Benutzer aktiviert sein](#)
- [\[IAM.21\] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen](#)
- [\[IAM.22\] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden](#)
- [\[IAM.23\] IAM Access Analyzer-Analysen sollten markiert werden](#)
- [\[IAM.24\] IAM-Rollen sollten mit Tags versehen werden](#)
- [\[IAM.25\] IAM-Benutzer sollten markiert werden](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[IAM.27\] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWS Cloud Shell Full Access](#)
- [\[IAM.28\] Der externe Zugriffsanalysator für IAM Access Analyzer sollte aktiviert sein](#)
- [\[Inspector.1\] Das EC2 Scannen mit Amazon Inspector sollte aktiviert sein](#)
- [\[Inspector.2\] Das Amazon Inspector ECR-Scannen sollte aktiviert sein](#)
- [\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)
- [\[Inspector.4\] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein](#)
- [\[IoT.1\] AWS IoT Device Defender Sicherheitsprofile sollten markiert werden](#)
- [\[IoT.2\] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden](#)
- [\[IoT.3\] AWS IoT Core -Dimensionen sollten markiert werden](#)
- [\[IoT.4\] AWS IoT Core Autorisierer sollten markiert werden](#)
- [\[IoT.5\] AWS IoT Core Rollenalias sollten markiert werden](#)

- [\[IoT.6\] AWS IoT Core Richtlinien sollten markiert werden](#)
- [\[IoTEvents .1\] AWS IoT-Events-Eingaben sollten markiert werden](#)
- [\[IoTEvents .2\] AWS IoT-Ereignisdetektormodelle sollten markiert werden](#)
- [\[IoTEvents .3\] Alarmmodelle für AWS IoT Events sollten markiert werden](#)
- [\[IoTSiteWise.1\] AWS SiteWise IoT-Asset-Modelle sollten markiert werden](#)
- [\[IoTSiteWise.2\] AWS SiteWise IoT-Dashboards sollten markiert werden](#)
- [\[IoTSiteWise.3\] AWS SiteWise IoT-Gateways sollten markiert werden](#)
- [\[IoTSiteWise.4\] AWS SiteWise IoT-Portale sollten markiert werden](#)
- [\[IoTSiteWise.5\] AWS SiteWise IoT-Projekte sollten markiert werden](#)
- [\[IoT TwinMaker.1\] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden](#)
- [\[IoT TwinMaker.2\] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden](#)
- [\[IoT TwinMaker.3\] AWS TwinMaker IoT-Szenen sollten markiert werden](#)
- [\[IoT TwinMaker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[IoTWireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[IoTWireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)
- [\[IoTWireless .3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)
- [\[Keyspaces.1\] Amazon Keyspaces Keyspaces sollten mit Tags versehen sein](#)
- [\[Kinesis.1\] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden](#)
- [\[Kinesis.2\] Kinesis-Streams sollten markiert werden](#)
- [\[Kinesis.3\] Kinesis-Streams sollten über eine angemessene Aufbewahrungsfrist für Daten verfügen](#)
- [\[KMS.1\] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)
- [\[KMS.2\] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)
- [\[KMS.5\] KMS-Schlüssel sollten nicht öffentlich zugänglich sein](#)
- [\[Lambda.5\] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren](#)
- [\[Lambda.7\] Bei Lambda-Funktionen sollte aktives Tracing aktiviert sein AWS X-Ray](#)

- [\[Macie.1\] Amazon Macie sollte aktiviert sein](#)
- [\[Macie.2\] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein](#)
- [\[MQ.2\] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch](#)
- [\[MQ.3\] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein](#)
- [\[MQ.4\] Amazon MQ-Broker sollten markiert werden](#)
- [\[MQ.5\] ActiveMQ-Broker sollten den Aktiv-/Standby-Bereitstellungsmodus verwenden](#)
- [\[MQ.6\] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden](#)
- [\[MSK.1\] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden](#)
- [\[MSK.2\] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein](#)
- [\[MSK.3\] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden](#)
- [\[MSK.4\] Bei MSK-Clustern sollte der öffentliche Zugriff deaktiviert sein](#)
- [\[MSK.5\] Bei MSK-Konnektoren sollte die Protokollierung aktiviert sein](#)
- [\[MSK.6\] MSK-Cluster sollten den nicht authentifizierten Zugriff deaktivieren](#)
- [\[Neptune.1\] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.2\] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)
- [\[Neptune.3\] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein](#)
- [\[Neptune.4\] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[Neptune.5\] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein](#)
- [\[Neptune.6\] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.7\] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein](#)
- [\[Neptune.8\] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren](#)
- [\[Neptune.9\] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden](#)
- [\[NetworkFirewall.1\] Network firewalls sollten über mehrere Availability Zones hinweg bereitgestellt werden](#)
- [\[NetworkFirewall.2\] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein](#)
- [\[NetworkFirewall.3\] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet haben](#)
- [\[NetworkFirewall.4\] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ sein.](#)
- [\[NetworkFirewall.5\] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ sein.](#)

- [\[NetworkFirewall.6\] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein](#)
- [\[NetworkFirewall.9\] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein](#)
- [\[NetworkFirewall.10\] Bei Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein](#)
- [Bei \[Opensearch.1\] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein](#)
- [\[Opensearch.2\] OpenSearch -Domains sollten nicht öffentlich zugänglich sein](#)
- [\[Opensearch.3\] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden](#)
- [Die Protokollierung von \[Opensearch.4\] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein](#)
- [Für \[Opensearch.5\] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein](#)
- [\[Opensearch.6\] OpenSearch Domains sollten mindestens drei Datenknoten haben](#)
- [Für \[Opensearch.7\] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein](#)
- [\[Opensearch.8\] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden](#)
- [\[Opensearch.9\] OpenSearch -Domains sollten mit Tags versehen werden](#)
- [Auf \[Opensearch.10\] OpenSearch -Domains sollte das neueste Softwareupdate installiert sein](#)
- [\[Opensearch.11\] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben](#)
- [\[PCA.1\] AWS Private CA Root-Zertifizierungsstelle sollte deaktiviert sein](#)
- [\[PCA.2\] AWS Private CA-Zertifizierungsstellen sollten gekennzeichnet werden](#)
- [\[RDS.14\] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein](#)
- [\[RDS.18\] RDS-Instances sollten in einer VPC bereitgestellt werden](#)
- [\[RDS.24\] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden](#)
- [\[RDS.25\] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden](#)
- [\[RDS.26\] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden](#)
- [\[RDS.27\] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[RDS.31\] RDS-DB-Sicherheitsgruppen sollten markiert werden](#)
- [\[RDS.34\] Aurora MySQL-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)

- [\[RDS.35\] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein](#)
- [\[RDS.36\] RDS für PostgreSQL-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[RDS.37\] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[RDS.38\] RDS für PostgreSQL-DB-Instances sollten bei der Übertragung verschlüsselt werden](#)
- [\[RDS.39\] RDS für MySQL-DB-Instances sollten bei der Übertragung verschlüsselt werden](#)
- [\[RDS.40\] RDS für SQL Server-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[RDS.41\] RDS für SQL Server-DB-Instances sollten bei der Übertragung verschlüsselt werden](#)
- [\[RDS.42\] RDS für MariaDB-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[RDS.44\] RDS für MariaDB-DB-Instances sollte bei der Übertragung verschlüsselt werden](#)
- [\[RDS.45\] Bei Aurora MySQL-DB-Clustern sollte die Audit-Protokollierung aktiviert sein](#)
- [\[Redshift.1\] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten](#)
- [\[Redshift.2\] Verbindungen zu Amazon Redshift Redshift-Clustern sollten bei der Übertragung verschlüsselt werden](#)
- [\[Redshift.3\] Bei Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein](#)
- [\[Redshift.4\] Bei Amazon Redshift Redshift-Clustern sollte die Auditprotokollierung aktiviert sein](#)
- [\[Redshift.6\] Bei Amazon Redshift sollten automatische Upgrades auf Hauptversionen aktiviert sein](#)
- [\[Redshift.7\] Redshift-Cluster sollten erweitertes VPC-Routing verwenden](#)
- [\[Redshift.8\] Amazon Redshift Redshift-Cluster sollten nicht den standardmäßigen Admin-Benutzernamen verwenden](#)
- [\[Redshift.9\] Redshift-Cluster sollten nicht den Standard-Datenbanknamen verwenden](#)
- [\[Redshift.10\] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[Redshift.11\] Redshift-Cluster sollten markiert werden](#)
- [\[Redshift.13\] Redshift-Cluster-Snapshots sollten markiert werden](#)
- [\[Redshift.15\] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen](#)
- [\[Redshift.16\] Redshift-Cluster-Subnetzgruppen sollten Subnetze aus mehreren Availability Zones haben](#)
- [\[Redshift.17\] Redshift-Cluster-Parametergruppen sollten markiert werden](#)
- [\[Redshift.18\] Für Redshift-Cluster sollten Multi-AZ-Bereitstellungen aktiviert sein](#)
- [\[RedshiftServerless.1\] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden](#)

- [\[RedshiftServerless.2\] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein](#)
- [\[RedshiftServerless.3\] Serverlose Redshift-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten](#)
- [\[RedshiftServerless.4\] Serverlose Redshift-Namespace sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys](#)
- [\[RedshiftServerless.5\] Redshift Serverless-Namespace sollten nicht den Standard-Admin-Benutzernamen verwenden](#)
- [\[RedshiftServerless.6\] Redshift Serverless Namespace sollten Protokolle in Logs exportieren CloudWatch](#)
- [\[RedshiftServerless.7\] Redshift Serverless-Namespace sollten nicht den Standard-Datenbanknamen verwenden](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.7\] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden](#)
- [\[S3.10\] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben](#)
- [\[S3.11\] Bei S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein](#)
- [\[S3.12\] ACLs sollte nicht zur Verwaltung des Benutzerzugriffs auf S3-Allzweck-Buckets verwendet werden](#)
- [\[S3.13\] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben](#)
- [\[S3.19\] Bei S3-Zugriffspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.20\] Bei S3-Allzweck-Buckets sollte MFA Delete aktiviert sein](#)
- [\[S3.22\] S3-Allzweck-Buckets sollten Schreibereignisse auf Objektebene protokollieren](#)
- [\[S3.23\] S3-Allzweck-Buckets sollten Leseereignisse auf Objektebene protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)
- [\[SageMaker.1\] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben](#)
- [\[SageMaker.2\] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden](#)
- [\[SageMaker.3\] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben](#)

- [\[SageMaker.4\] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein](#)
- [\[SageMaker.5\] SageMaker Modelle sollten eingehenden Datenverkehr blockieren](#)
- [\[SageMaker.6\] SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden](#)
- [\[SageMaker.7\] SageMaker Bilder sollten mit Tags versehen werden](#)
- [\[SageMaker.8\] SageMaker Notebook-Instances sollten auf unterstützten Plattformen laufen](#)
- [\[SES.1\] SES-Kontaktlisten sollten mit Tags versehen werden](#)
- [\[SES.2\] SES-Konfigurationssätze sollten mit Tags versehen werden](#)
- [\[ServiceCatalog.1\] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden](#)
- [\[SNS.4\] Zugriffsrichtlinien für SNS-Themen sollten keinen öffentlichen Zugriff zulassen](#)
- [\[SQS.1\] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt werden](#)
- [\[SQS.2\] SQS-Warteschlangen sollten markiert werden](#)
- [\[SQS.3\] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen](#)
- [\[SSM.3\] Von Systems Manager verwaltete EC2 Amazon-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben](#)
- [\[SSM.4\] SSM-Dokumente sollten nicht öffentlich sein](#)
- [\[SSM.5\] SSM-Dokumente sollten mit Tags versehen werden](#)
- [\[SSM.6\] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[SSM.7\] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein](#)
- [\[StepFunctions.1\] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben](#)
- [\[StepFunctions.2\] Die Aktivitäten von Step Functions sollten mit Tags versehen werden](#)
- [\[Transfer.1\] AWS Transfer Family -Workflows sollten mit Tags versehen werden](#)
- [\[Transfer.2\] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden](#)
- [\[Transfer.3\] Bei Connectoren der Transfer-Familie sollte die Protokollierung aktiviert sein](#)
- [\[Transfer.4\] Transfer Family Familienverträge sollten gekennzeichnet werden](#)
- [\[Transfer.5\] Transfer Family Familienzertifikate sollten gekennzeichnet sein](#)
- [\[Transfer.6\] Steckverbinder der Transfer-Familie sollten gekennzeichnet sein](#)

- [\[Transfer.7\] Familienprofile sollten mit Tags versehen werden](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.2\] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.3\] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.4\] AWS WAF Classic Regional Web ACLs sollte mindestens eine Regel oder Regelgruppe enthalten](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WAF.10\] AWS WAF web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [Für \[WAF.12\] AWS WAF Regeln sollten Metriken aktiviert sein CloudWatch](#)
- [\[WorkSpaces.1\] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden](#)
- [\[WorkSpaces.2\] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden](#)

Asien-Pazifik (Melbourne)

Die folgenden Steuerelemente werden in der Region Asien-Pazifik (Melbourne) nicht unterstützt.

- [\[APIGateway.8\] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben](#)
- [\[APIGateway.9\] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein](#)
- [\[Amplify.1\] Amplify-Apps sollten markiert werden](#)
- [\[Amplify.2\] Amplify-Zweige sollten markiert werden](#)
- [\[AppFlow.1\] AppFlow Amazon-Datenflüsse sollten mit Tags versehen werden](#)
- [\[AppRunner.1\] App Runner-Dienste sollten markiert sein](#)
- [\[AppRunner.2\] App Runner VPC-Konnektoren sollten markiert sein](#)
- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.2\] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben](#)
- [\[AppSync.5\] AWS AppSync GraphQL APIs sollte nicht mit API-Schlüsseln authentifiziert werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [\[Backup.1\] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein](#)

- [\[Backup.4\] AWS Backup Berichtspläne sollten markiert werden](#)
- [\[Batch.1\] Warteschlangen für Batch-Jobs sollten markiert werden](#)
- [\[Batch.3\] Batch-Computing-Umgebungen sollten markiert werden](#)
- [\[Batch.4\] Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[CodeArtifact.1\] CodeArtifact Repositorien sollten mit Tags versehen werden](#)
- [\[CodeGuruProfiler.1\] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden](#)
- [\[CodeGuruReviewer.1\] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden](#)
- [\[Cognito.1\] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein](#)
- [\[Connect.1\] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden](#)
- [\[Connect.2\] Für Amazon Connect Connect-Instances sollte die Protokollierung aktiviert sein CloudWatch](#)

- [\[Detective.1\] Verhaltensdiagramme von Detektiven sollten markiert werden](#)
- [\[DMS.2\] DMS-Zertifikate sollten gekennzeichnet sein](#)
- [\[DMS.3\] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden](#)
- [\[DMS.4\] DMS-Replikationsinstanzen sollten markiert werden](#)
- [\[DMS.5\] Subnetzgruppen für die DMS-Replikation sollten markiert werden](#)
- [\[DMS.6\] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein](#)
- [\[DMS.7\] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.8\] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.9\] DMS-Endpunkte sollten SSL verwenden](#)
- [\[DMS.10\] Bei DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein](#)
- [\[DMS.11\] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein](#)
- [\[DMS.12\] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein](#)
- [\[DocumentDB.1\] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DocumentDB.2\] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen](#)
- [\[DocumentDB.3\] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein](#)
- [\[DocumentDB.4\] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch](#)
- [\[DocumentDB.5\] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[DocumentDB.6\] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[DynamoDB.3\] DynamoDB Accelerator \(DAX\) -Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DynamoDB.4\] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein](#)
- [\[DynamoDB.7\] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[EC2.1\] Amazon EBS-Snapshots sollten nicht öffentlich wiederherstellbar sein](#)
- [\[EC2.4\] Gestoppte EC2 Instances sollten nach einem bestimmten Zeitraum entfernt werden](#)

- [\[EC2.8\] EC2 Instances sollten Instance Metadata Service Version 2 \(\) verwenden IMDSv2](#)
- [\[EC2.14\] Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 oder: :/0 auf Port 3389 zulassen](#)
- [\[EC2.18\] Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Datenverkehr für autorisierte Ports zulassen](#)
- [\[EC2.22\] Ungenutzte EC2 Amazon-Sicherheitsgruppen sollten entfernt werden](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways sollte VPC-Anhangsanfragen nicht automatisch akzeptieren](#)
- [\[EC2.24\] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden](#)
- [\[EC2.25\] EC2 Amazon-Startvorlagen sollten Netzwerkschnittstellen nicht öffentlich IPs zuweisen](#)
- [\[EC2.28\] EBS-Volumes sollten durch einen Backup-Plan abgedeckt sein](#)
- [\[EC2.34\] Die Routentabellen für EC2 Transit-Gateways sollten mit Tags versehen werden](#)
- [\[EC2.40\] EC2 NAT-Gateways sollten markiert werden](#)
- [\[EC2.48\] Amazon VPC-Flow-Logs sollten mit Tags versehen werden](#)
- [\[EC2.58\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert sein](#)
- [\[EC2.60\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden](#)
- [\[EC2.170\] EC2 Startvorlagen sollten Instance Metadata Service Version 2 \(\) verwenden IMDSv2](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[EC2.175\] EC2 Startvorlagen sollten mit Tags versehen sein](#)
- [\[ECR.4\] Öffentliche ECR-Repositoryn sollten markiert werden](#)
- [\[EFS.1\] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS](#)
- [\[EFS.2\] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein](#)
- [\[ELB.14\] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden](#)
- [\[ELB.17\] Anwendungs- und Netzwerk-Load-Balancer mit Listnern sollten die empfohlenen Sicherheitsrichtlinien verwenden](#)
- [\[ELB.18\] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln](#)
- [Bei \[ElastiCache.1\] ElastiCache \(Redis OSS\) -Clustern sollten automatische Backups aktiviert sein](#)

- [\[ElastiCache.2\] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein](#)
- [\[ElastiCache.3\] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein](#)
- [\[ElastiCache.4\] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden](#)
- [\[ElastiCache.5\] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden](#)
- [\[ElastiCache.6\] Für Replikationsgruppen ElastiCache \(Redis OSS\) früherer Versionen sollte Redis OSS AUTH aktiviert sein](#)
- [\[ElastiCache.7\] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden](#)
- [\[ElasticBeanstalk.1\] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben](#)
- [\[ElasticBeanstalk.2\] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk sollte Logs streamen nach CloudWatch](#)
- [\[EMR.1\] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben](#)
- [\[ES.4\] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein](#)
- [\[EventBridge.4\] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[FSx.1\] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden](#)
- [\[FSx.3\] FSx für OpenZFS-Dateisysteme sollte für die Multi-AZ-Bereitstellung konfiguriert werden](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[Glue.4\] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue](#)
- [\[GuardDuty.2\] GuardDuty Filter sollten mit Tags versehen sein](#)
- [\[IAM.1\] IAM-Richtlinien sollten keine vollen „*“-Administratorrechte zulassen](#)
- [\[IAM.2\] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein](#)
- [\[IAM.3\] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden](#)
- [\[IAM.5\] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen](#)

- [\[IAM.6\] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.](#)
- [\[IAM.8\] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden](#)
- [\[IAM.10\] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein](#)
- [\[IAM.11\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert](#)
- [\[IAM.12\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert](#)
- [\[IAM.13\] Stellen Sie sicher, dass für die IAM-Passwortrichtlinie mindestens ein Symbol erforderlich ist](#)
- [\[IAM.14\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert](#)
- [\[IAM.15\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert](#)
- [\[IAM.16\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert](#)
- [\[IAM.17\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft](#)
- [\[IAM.18\] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS -Support](#)
- [\[IAM.19\] MFA sollte für alle IAM-Benutzer aktiviert sein](#)
- [\[IAM.21\] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen](#)
- [\[IAM.22\] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden](#)
- [\[IAM.24\] IAM-Rollen sollten mit Tags versehen werden](#)
- [\[IAM.25\] IAM-Benutzer sollten markiert werden](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[IAM.27\] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloud ShellFullAccess](#)
- [\[Inspector.1\] Das EC2 Scannen mit Amazon Inspector sollte aktiviert sein](#)
- [\[Inspector.2\] Das Amazon Inspector ECR-Scannen sollte aktiviert sein](#)
- [\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)
- [\[Inspector.4\] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein](#)
- [\[IoT.1\] AWS IoT Device Defender Sicherheitsprofile sollten markiert werden](#)

- [\[IoT.2\] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden](#)
- [\[IoT.3\] AWS IoT Core -Dimensionen sollten markiert werden](#)
- [\[IoT.4\] AWS IoT Core Autorisierer sollten markiert werden](#)
- [\[IoT.5\] AWS IoT Core Rollenalias sollten markiert werden](#)
- [\[IoT.6\] AWS IoT Core Richtlinien sollten markiert werden](#)
- [\[IoTEvents .1\] AWS IoT-Events-Eingaben sollten markiert werden](#)
- [\[IoTEvents .2\] AWS IoT-Ereignisdetektormodelle sollten markiert werden](#)
- [\[IoTEvents .3\] Alarmmodelle für AWS IoT Events sollten markiert werden](#)
- [\[IoTSiteWise.1\] AWS SiteWise IoT-Asset-Modelle sollten markiert werden](#)
- [\[IoTSiteWise.2\] AWS SiteWise IoT-Dashboards sollten markiert werden](#)
- [\[IoTSiteWise.3\] AWS SiteWise IoT-Gateways sollten markiert werden](#)
- [\[IoTSiteWise.4\] AWS SiteWise IoT-Portale sollten markiert werden](#)
- [\[IoTSiteWise.5\] AWS SiteWise IoT-Projekte sollten markiert werden](#)
- [\[IoTtwinmaker.1\] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden](#)
- [\[IoTtwinmaker.2\] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden](#)
- [\[IoTtwinmaker.3\] AWS TwinMaker IoT-Szenen sollten markiert werden](#)
- [\[IoTtwinmaker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[IoTWireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[IoTWireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)
- [\[IoTWireless .3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)
- [\[Keyspaces.1\] Amazon Keyspaces Keyspaces sollten mit Tags versehen sein](#)
- [\[Kinesis.1\] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden](#)
- [\[KMS.1\] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)
- [\[KMS.2\] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)
- [\[Macie.1\] Amazon Macie sollte aktiviert sein](#)

- [\[Macie.2\] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein](#)
- [\[MQ.6\] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden](#)
- [\[MSK.3\] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden](#)
- [\[MSK.5\] Bei MSK-Konnektoren sollte die Protokollierung aktiviert sein](#)
- [\[Neptune.1\] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.2\] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)
- [\[Neptune.3\] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein](#)
- [\[Neptune.4\] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[Neptune.5\] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein](#)
- [\[Neptune.6\] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.7\] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein](#)
- [\[Neptune.8\] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren](#)
- [\[Neptune.9\] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden](#)
- [Bei \[Opensearch.1\] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein](#)
- [\[Opensearch.2\] OpenSearch -Domains sollten nicht öffentlich zugänglich sein](#)
- [\[Opensearch.3\] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden](#)
- [Die Protokollierung von \[Opensearch.4\] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein](#)
- [Für \[Opensearch.5\] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein](#)
- [\[Opensearch.6\] OpenSearch Domains sollten mindestens drei Datenknoten haben](#)
- [Für \[Opensearch.7\] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein](#)
- [\[Opensearch.8\] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden](#)
- [\[Opensearch.9\] OpenSearch -Domains sollten mit Tags versehen werden](#)
- [Auf \[Opensearch.10\] OpenSearch -Domains sollte das neueste Softwareupdate installiert sein](#)
- [\[Opensearch.11\] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben](#)
- [\[RDS.1\] Der RDS-Snapshot sollte privat sein](#)
- [\[RDS.14\] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein](#)

- [\[RDS.15\] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden](#)
- [\[RDS.26\] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden](#)
- [\[RDS.31\] RDS-DB-Sicherheitsgruppen sollten markiert werden](#)
- [\[RDS.35\] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein](#)
- [\[RDS.37\] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[RedshiftServerless.1\] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden](#)
- [\[RedshiftServerless.2\] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein](#)
- [\[RedshiftServerless.3\] Serverlose Redshift-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten](#)
- [\[RedshiftServerless.4\] Serverlose Redshift-Namespaces sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys](#)
- [\[RedshiftServerless.5\] Redshift Serverless-Namespaces sollten nicht den Standard-Admin-Benutzernamen verwenden](#)
- [\[RedshiftServerless.6\] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch](#)
- [\[RedshiftServerless.7\] Redshift Serverless-Namespaces sollten nicht den Standard-Datenbanknamen verwenden](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)
- [\[SageMaker.1\] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben](#)
- [\[SageMaker.2\] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden](#)
- [\[SageMaker.3\] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben](#)
- [\[SageMaker.5\] SageMaker Modelle sollten eingehenden Datenverkehr blockieren](#)
- [\[SageMaker.6\] SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden](#)
- [\[SageMaker.7\] SageMaker Bilder sollten mit Tags versehen werden](#)
- [\[SageMaker.8\] SageMaker Notebook-Instances sollten auf unterstützten Plattformen laufen](#)

- [\[SES.1\] SES-Kontaktlisten sollten mit Tags versehen werden](#)
- [\[SES.2\] SES-Konfigurationssätze sollten mit Tags versehen werden](#)
- [\[SQS.1\] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt werden](#)
- [\[SQS.2\] SQS-Warteschlangen sollten markiert werden](#)
- [\[SQS.3\] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen](#)
- [\[SSM.3\] Von Systems Manager verwaltete EC2 Amazon-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben](#)
- [\[SSM.4\] SSM-Dokumente sollten nicht öffentlich sein](#)
- [\[SSM.7\] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein](#)
- [\[StepFunctions.1\] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben](#)
- [\[Transfer.3\] Bei Connectoren der Transfer-Familie sollte die Protokollierung aktiviert sein](#)
- [\[Transfer.4\] Transfer Family Familienverträge sollten gekennzeichnet werden](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WAF.11\] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WorkSpaces.1\] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden](#)
- [\[WorkSpaces.2\] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden](#)

Asien-Pazifik (Mumbai)

Die folgenden Steuerelemente werden in der Region Asien-Pazifik (Mumbai) nicht unterstützt.

- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)

- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[CodeGuruProfiler.1\] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden](#)
- [\[CodeGuruReviewer.1\] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden](#)
- [\[Connect.1\] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden](#)
- [\[Connect.2\] Für Amazon Connect Connect-Instances sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[EC2.24\] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[ECR.4\] Öffentliche ECR-Repositories sollten markiert werden](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)

- [\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)
- [\[IoT Twin Maker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[IoT Wireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[IoT Wireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)
- [\[IoT Wireless .3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[RDS.31\] RDS-DB-Sicherheitsgruppen sollten markiert werden](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)

Asien-Pazifik (Osaka)

Die folgenden Steuerelemente werden in der Region Asien-Pazifik (Osaka) nicht unterstützt.

- [\[ACM.1\] Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden](#)
- [\[AppFlow.1\] AppFlow Amazon-Datenflüsse sollten mit Tags versehen werden](#)
- [\[AppRunner.1\] App Runner-Dienste sollten markiert sein](#)
- [\[AppRunner.2\] App Runner VPC-Konnektoren sollten markiert sein](#)
- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [\[Backup.1\] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein](#)
- [\[Backup.4\] AWS Backup Berichtspläne sollten markiert werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)

- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[CodeArtifact.1\] CodeArtifact Repositorien sollten mit Tags versehen werden](#)
- [\[CodeGuruProfiler.1\] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden](#)
- [\[CodeGuruReviewer.1\] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden](#)
- [\[Connect.1\] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden](#)
- [\[Connect.2\] Für Amazon Connect Connect-Instances sollte die Protokollierung aktiviert sein](#)
[CloudWatch](#)
- [\[Detective.1\] Verhaltensdiagramme von Detektiven sollten markiert werden](#)
- [\[DMS.7\] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.8\] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.10\] Bei DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein](#)
- [\[DocumentDB.1\] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DocumentDB.2\] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen](#)

- [\[DocumentDB.3\] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein](#)
- [\[DocumentDB.4\] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch](#)
- [\[DocumentDB.5\] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[DocumentDB.6\] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[DynamoDB.3\] DynamoDB Accelerator \(DAX\) -Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DynamoDB.7\] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[EC2.4\] Gestoppte EC2 Instances sollten nach einem bestimmten Zeitraum entfernt werden](#)
- [\[EC2.8\] EC2 Instances sollten Instance Metadata Service Version 2 \(\) verwenden IMDSv2](#)
- [\[EC2.14\] Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 oder: :/0 auf Port 3389 zulassen](#)
- [\[EC2.20\] Beide VPN-Tunnel für eine AWS Site-to-Site VPN-Verbindung sollten aktiv sein](#)
- [\[EC2.22\] Ungenutzte EC2 Amazon-Sicherheitsgruppen sollten entfernt werden](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways sollte VPC-Anhangsanfragen nicht automatisch akzeptieren](#)
- [\[EC2.24\] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden](#)
- [\[EC2.55\] VPCs sollte mit einem Schnittstellenendpunkt für die ECR-API konfiguriert werden](#)
- [\[EC2.56\] VPCs sollte mit einem Schnittstellenendpunkt für Docker Registry konfiguriert werden](#)
- [\[EC2.57\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager konfiguriert werden](#)
- [\[EC2.58\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert sein](#)
- [\[EC2.60\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[ECR.4\] Öffentliche ECR-Repositoryn sollten markiert werden](#)
- [\[ELB.1\] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden](#)
- [\[ELB.2\] Classic Load Balancer mit SSL/HTTPS Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager](#)

- [\[ELB.3\] Classic Load Balancer Listener sollten mit HTTPS- oder TLS-Terminierung konfiguriert werden](#)
- [\[ELB.4\] Application Load Balancer sollte so konfiguriert sein, dass ungültige HTTP-Header gelöscht werden](#)
- [\[ELB.6\] Für Anwendungen, Gateways und Network Load Balancers sollte der Löschschutz aktiviert sein](#)
- [\[ELB.8\] Classic Load Balancer mit SSL-Listnern sollten eine vordefinierte Sicherheitsrichtlinie mit starker Dauer verwenden AWS Config](#)
- [\[ELB.16\] Application Load Balancers sollten mit einer Web-ACL verknüpft sein AWS WAF](#)
- [Bei \[ElastiCache.1\] ElastiCache \(Redis OSS\) -Clustern sollten automatische Backups aktiviert sein](#)
- [\[ElastiCache.7\] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden](#)
- [\[ElasticBeanstalk.1\] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben](#)
- [\[ElasticBeanstalk.2\] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein](#)
- [\[EMR.1\] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[IAM.4\] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren](#)
- [\[IAM.18\] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS -Support](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)
- [\[IoT.1\] AWS IoT Device Defender Sicherheitsprofile sollten markiert werden](#)
- [\[IoT.2\] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden](#)
- [\[IoT.3\] AWS IoT Core -Dimensionen sollten markiert werden](#)
- [\[IoT.4\] AWS IoT Core Autorisierer sollten markiert werden](#)
- [\[IoT.5\] AWS IoT Core Rollenalias sollten markiert werden](#)
- [\[IoT.6\] AWS IoT Core Richtlinien sollten markiert werden](#)

- [\[Io TEvents .1\] AWS IoT-Events-Eingaben sollten markiert werden](#)
- [\[Io TEvents .2\] AWS IoT-Ereignisdetektormodelle sollten markiert werden](#)
- [\[Io TEvents .3\] Alarmmodelle für AWS IoT Events sollten markiert werden](#)
- [\[Io TSite Wise.1\] AWS SiteWise IoT-Asset-Modelle sollten markiert werden](#)
- [\[Io TSite Wise.2\] AWS SiteWise IoT-Dashboards sollten markiert werden](#)
- [\[Io TSite Wise.3\] AWS SiteWise IoT-Gateways sollten markiert werden](#)
- [\[Io TSite Wise.4\] AWS SiteWise IoT-Portale sollten markiert werden](#)
- [\[Io TSite Wise.5\] AWS SiteWise IoT-Projekte sollten markiert werden](#)
- [\[Io TTwin Maker.1\] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden](#)
- [\[Io TTwin Maker.2\] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden](#)
- [\[Io TTwin Maker.3\] AWS TwinMaker IoT-Szenen sollten markiert werden](#)
- [\[Io TTwin Maker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[Io TWireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[Io TWireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)
- [\[Io TWireless .3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)
- [\[Keyspaces.1\] Amazon Keyspaces Keyspaces sollten mit Tags versehen sein](#)
- [\[MSK.3\] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden](#)
- [\[MSK.5\] Bei MSK-Konnektoren sollte die Protokollierung aktiviert sein](#)
- [\[RDS.31\] RDS-DB-Sicherheitsgruppen sollten markiert werden](#)
- [\[RedshiftServerless.1\] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden](#)
- [\[RedshiftServerless.2\] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein](#)
- [\[RedshiftServerless.3\] Serverlose Redshift-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten](#)
- [\[RedshiftServerless.4\] Serverlose Redshift-Namespace sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys](#)
- [\[RedshiftServerless.5\] Redshift Serverless-Namespace sollten nicht den Standard-Admin-Benutzernamen verwenden](#)

- [\[RedshiftServerless.6\] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch](#)
- [\[RedshiftServerless.7\] Redshift Serverless-Namespaces sollten nicht den Standard-Datenbanknamen verwenden](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)
- [\[SSM.2\] Von Systems Manager verwaltete EC2 Amazon-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben](#)
- [\[SSM.3\] Von Systems Manager verwaltete EC2 Amazon-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.3\] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WAF.10\] AWS WAF web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WAF.11\] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WorkSpaces.1\] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden](#)
- [\[WorkSpaces.2\] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden](#)

Asien-Pazifik (Seoul)

Die folgenden Steuerelemente werden in der Region Asien-Pazifik (Seoul) nicht unterstützt.

- [\[AppRunner.1\] App Runner-Dienste sollten markiert sein](#)
- [\[AppRunner.2\] App Runner VPC-Konnektoren sollten markiert sein](#)
- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)

- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[CodeArtifact.1\] CodeArtifact Repositorien sollten mit Tags versehen werden](#)
- [\[CodeGuruProfiler.1\] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden](#)
- [\[CodeGuruReviewer.1\] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden](#)
- [\[Cognito.2\] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen](#)
- [\[DynamoDB.3\] DynamoDB Accelerator \(DAX\) -Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DynamoDB.7\] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[EC2.24\] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[EC2.180\] Bei EC2 Netzwerkschnittstellen sollte die source/destination Überprüfung aktiviert sein](#)
- [\[ECR.4\] Öffentliche ECR-Repositorien sollten markiert werden](#)

- [\[ELB.18\] Anwendungs- und Network Load Balancer Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[Glue.4\] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)
- [\[IoT Twin Maker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[IoT Wireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[IoT Wireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)
- [\[IoT Wireless .3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[Lambda.7\] Bei Lambda-Funktionen sollte aktives Tracing aktiviert sein AWS X-Ray](#)
- [\[MSK.4\] Bei MSK-Clustern sollte der öffentliche Zugriff deaktiviert sein](#)
- [\[MSK.5\] Bei MSK-Konnektoren sollte die Protokollierung aktiviert sein](#)
- [\[MSK.6\] MSK-Cluster sollten den nicht authentifizierten Zugriff deaktivieren](#)
- [\[RDS.31\] RDS-DB-Sicherheitsgruppen sollten markiert werden](#)
- [\[Redshift.18\] Für Redshift-Cluster sollten Multi-AZ-Bereitstellungen aktiviert sein](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)
- [\[SSM.6\] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[SSM.7\] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)

- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)

Asien-Pazifik (Singapur)

Die folgenden Steuerelemente werden in der Region Asien-Pazifik (Singapur) nicht unterstützt.

- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[ECR.4\] Öffentliche ECR-Repositorien sollten markiert werden](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)

- [\[Io TWireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[Io TWireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)
- [\[Io TWireless .3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)

Asien-Pazifik (Sydney)

Die folgenden Steuerelemente werden in der Region Asien-Pazifik (Sydney) nicht unterstützt.

- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)

- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[ECR.4\] Öffentliche ECR-Repositoryn sollten markiert werden](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)

Asien-Pazifik (Taipeh)

Die folgenden Steuerelemente werden in der Region Asien-Pazifik (Taipeh) nicht unterstützt.

- [\[ACM.1\] Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden](#)
- [\[ACM.2\] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden](#)
- [\[ACM.3\] ACM-Zertifikate sollten mit einem Tag versehen werden](#)
- [\[Account.1\] Sicherheitskontaktinformationen sollten bereitgestellt werden für AWS-Konto](#)
- [\[Account.2\] AWS-Konten sollte Teil einer Organisation sein AWS Organizations](#)
- [\[APIGateway.1\] API Gateway REST und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein](#)
- [\[APIGateway.2\] API Gateway REST API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden](#)
- [\[APIGateway.3\] Bei den REST-API-Stufen von API Gateway sollte die AWS X-Ray Ablaufverfolgung aktiviert sein](#)
- [\[APIGateway.4\] API Gateway sollte mit einer WAF-Web-ACL verknüpft sein](#)
- [\[APIGateway.5\] API Gateway REST API-Cache-Daten sollten im Ruhezustand verschlüsselt werden](#)
- [\[APIGateway.8\] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben](#)
- [\[APIGateway.9\] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein](#)
- [\[Amplify.1\] Amplify-Apps sollten markiert werden](#)
- [\[Amplify.2\] Amplify-Zweige sollten markiert werden](#)
- [\[AppConfig.1\] AWS AppConfig Anwendungen sollten markiert werden](#)
- [\[AppConfig.2\] AWS AppConfig Konfigurationsprofile sollten mit Tags versehen werden](#)
- [\[AppConfig.3\] AWS AppConfig Umgebungen sollten markiert werden](#)
- [\[AppConfig.4\] AWS AppConfig Erweiterungszuordnungen sollten markiert werden](#)
- [\[AppFlow.1\] AppFlow Amazon-Datenflüsse sollten mit Tags versehen werden](#)
- [\[AppRunner.1\] App Runner-Dienste sollten markiert sein](#)
- [\[AppRunner.2\] App Runner VPC-Konnektoren sollten markiert sein](#)
- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.2\] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben](#)
- [\[AppSync.4\] AWS AppSync GraphQL APIs sollte markiert sein](#)
- [\[AppSync.5\] AWS AppSync GraphQL APIs sollte nicht mit API-Schlüsseln authentifiziert werden](#)

- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [\[Athena.2\] Athena-Datenkataloge sollten mit Tags versehen werden](#)
- [\[Athena.3\] Athena-Arbeitsgruppen sollten markiert werden](#)
- [\[Athena.4\] Bei Athena-Arbeitsgruppen sollte die Protokollierung aktiviert sein](#)
- [\[AutoScaling.1\] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden](#)
- [\[AutoScaling.2\] Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken](#)
- [\[AutoScaling.3\] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2 Instances so konfigurieren, dass sie Instance Metadata Service Version 2 \(IMDSv2\) benötigen](#)
- [\[AutoScaling.6\] Auto Scaling Scaling-Gruppen sollten mehrere Instance-Typen in mehreren Availability Zones verwenden](#)
- [\[AutoScaling.9\] Amazon EC2 Auto Scaling Scaling-Gruppen sollten EC2 Amazon-Startvorlagen verwenden](#)
- [\[AutoScaling.10\] EC2 Auto Scaling Scaling-Gruppen sollten markiert werden](#)
- [\[Autoscaling.5\] EC2 Amazon-Instances, die mit Auto Scaling Scaling-Gruppenstartkonfigurationen gestartet wurden, sollten keine öffentlichen IP-Adressen haben](#)
- [\[Backup.1\] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein](#)
- [\[Backup.2\] AWS Backup Wiederherstellungspunkte sollten markiert werden](#)
- [\[Backup.3\] AWS Backup Tresore sollten markiert sein](#)
- [\[Backup.4\] AWS Backup Berichtspläne sollten markiert werden](#)
- [\[Backup.5\] AWS Backup Backup-Pläne sollten markiert werden](#)
- [\[Batch.1\] Warteschlangen für Batch-Jobs sollten markiert werden](#)
- [\[Batch.2\] Richtlinien für die Batch-Planung sollten gekennzeichnet sein](#)
- [\[Batch.3\] Batch-Computing-Umgebungen sollten markiert werden](#)
- [\[Batch.4\] Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden](#)
- [\[CloudFormation.2\] CloudFormation Stapel sollten markiert werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)

- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[CloudTrail.6\] Sicherstellen, dass der S3-Bucket, in dem CloudTrail Protokolle gespeichert werden, nicht öffentlich zugänglich ist](#)
- [\[CloudTrail.7\] Sicherstellen, dass die S3-Bucket-Zugriffsprotokollierung für den CloudTrail S3-Bucket aktiviert ist](#)
- [\[CloudTrail.9\] CloudTrail Pfade sollten markiert werden](#)
- [\[CloudTrail.10\] Event-Datenspeicher in CloudTrail Lake sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys](#)
- [\[CloudWatch.17\] CloudWatch Alarmaktionen sollten aktiviert sein](#)
- [\[CodeArtifact.1\] CodeArtifact Repositorien sollten mit Tags versehen werden](#)
- [\[CodeBuild.1\] Das CodeBuild Bitbucket-Quell-Repository URLs sollte keine vertraulichen Anmeldeinformationen enthalten](#)
- [\[CodeBuild.2\] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten](#)
- [\[CodeBuild.3\] CodeBuild S3-Protokolle sollten verschlüsselt sein](#)
- [\[CodeBuild.4\] CodeBuild Projektumgebungen sollten eine AWS Config Protokollierungsdauer haben](#)

- [\[CodeBuild.7\] Exporte von CodeBuild Berichtsgruppen sollten im Ruhezustand verschlüsselt werden](#)
- [\[CodeGuruProfiler.1\] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden](#)
- [\[CodeGuruReviewer.1\] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden](#)
- [\[Cognito.1\] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein](#)
- [\[Cognito.2\] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen](#)
- [\[Connect.1\] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden](#)
- [\[Connect.2\] Für Amazon Connect Connect-Instances sollte die Protokollierung aktiviert sein](#)
[CloudWatch](#)
- [\[DataFirehose.1\] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden](#)
- [\[DataSync.1\] Für DataSync Aufgaben sollte die Protokollierung aktiviert sein](#)
- [\[DataSync.2\] DataSync Aufgaben sollten mit Tags versehen werden](#)
- [\[Detective.1\] Verhaltensdiagramme von Detektiven sollten markiert werden](#)
- [\[DMS.1\] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein](#)
- [\[DMS.2\] DMS-Zertifikate sollten gekennzeichnet sein](#)
- [\[DMS.3\] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden](#)
- [\[DMS.4\] DMS-Replikationsinstanzen sollten markiert werden](#)
- [\[DMS.5\] Subnetzgruppen für die DMS-Replikation sollten markiert werden](#)
- [\[DMS.6\] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein](#)
- [\[DMS.7\] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.8\] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.9\] DMS-Endpunkte sollten SSL verwenden](#)
- [\[DMS.10\] Bei DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein](#)
- [\[DMS.11\] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein](#)
- [\[DMS.12\] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein](#)

- [\[DocumentDB.1\] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DocumentDB.2\] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen](#)
- [\[DocumentDB.3\] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein](#)
- [\[DocumentDB.4\] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch](#)
- [\[DocumentDB.5\] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[DocumentDB.6\] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[DynamoDB.3\] DynamoDB Accelerator \(DAX\) -Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DynamoDB.4\] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein](#)
- [\[DynamoDB.5\] DynamoDB-Tabellen sollten mit Tags versehen werden](#)
- [\[DynamoDB.6\] Bei DynamoDB-Tabellen sollte der Löschschutz aktiviert sein](#)
- [\[DynamoDB.7\] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[EC2.4\] Gestoppte EC2 Instances sollten nach einem bestimmten Zeitraum entfernt werden](#)
- [\[EC2.10\] Amazon EC2 sollte so konfiguriert sein, dass es VPC-Endpunkte verwendet, die für den Amazon-Service erstellt wurden EC2](#)
- [\[EC2.19\] Sicherheitsgruppen sollten keinen uneingeschränkten Zugriff auf Ports mit hohem Risiko zulassen](#)
- [\[EC2.21\] Das Netzwerk ACLs sollte keinen Zugang von 0.0.0.0/0 zu Port 22 oder Port 3389 zulassen](#)
- [\[EC2.22\] Ungenutzte EC2 Amazon-Sicherheitsgruppen sollten entfernt werden](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways sollte VPC-Anhangsanfragen nicht automatisch akzeptieren](#)
- [\[EC2.24\] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden](#)
- [\[EC2.25\] EC2 Amazon-Startvorlagen sollten Netzwerkschnittstellen nicht öffentlich IPs zuweisen](#)
- [\[EC2.28\] EBS-Volumes sollten durch einen Backup-Plan abgedeckt sein](#)
- [\[EC2.33\] EC2 Transit-Gateway-Anhänge sollten mit Tags versehen werden](#)
- [\[EC2.34\] Die Routentabellen für EC2 Transit-Gateways sollten mit Tags versehen werden](#)
- [\[EC2.35\] EC2 Netzwerkschnittstellen sollten markiert werden](#)
- [\[EC2.36\] EC2 Kunden-Gateways sollten mit Tags versehen werden](#)

- [\[EC2.37\] EC2 Elastische IP-Adressen sollten mit Tags versehen werden](#)
- [\[EC2.38\] EC2 Instances sollten markiert werden](#)
- [\[EC2.39\] EC2 Internet-Gateways sollten markiert werden](#)
- [\[EC2.40\] EC2 NAT-Gateways sollten markiert werden](#)
- [\[EC2.41\] Das EC2 Netzwerk ACLs sollte markiert sein](#)
- [\[EC2.42\] EC2 Routing-Tabellen sollten mit Tags versehen werden](#)
- [\[EC2.43\] EC2 Sicherheitsgruppen sollten markiert werden](#)
- [\[EC2.44\] EC2 Subnetze sollten markiert werden](#)
- [\[EC2.45\] EC2 Volumen sollten mit Tags versehen werden](#)
- [\[EC2.46\] Amazon VPCs sollte markiert werden](#)
- [\[EC2.47\] Amazon VPC Endpoint Services sollten markiert werden](#)
- [\[EC2.48\] Amazon VPC-Flow-Logs sollten mit Tags versehen werden](#)
- [\[EC2.49\] Amazon VPC-Peering-Verbindungen sollten markiert werden](#)
- [\[EC2.50\] EC2 VPN-Gateways sollten markiert werden](#)
- [\[EC2.51\] EC2 Client-VPN-Endpunkte sollten die Client-Verbindungsprotokollierung aktiviert haben](#)
- [\[EC2.52\] EC2 Transit-Gateways sollten markiert werden](#)
- [\[EC2.53\] EC2 Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 zu Remote-Serververwaltungsports zulassen](#)
- [\[EC2.54\] EC2 Sicherheitsgruppen sollten keinen Zugriff von: :/0 zu Remote-Serveradministrationsports zulassen](#)
- [\[EC2.55\] VPCs sollte mit einem Schnittstellenendpunkt für die ECR-API konfiguriert werden](#)
- [\[EC2.56\] VPCs sollte mit einem Schnittstellenendpunkt für Docker Registry konfiguriert werden](#)
- [\[EC2.57\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager konfiguriert werden](#)
- [\[EC2.58\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert sein](#)
- [\[EC2.60\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden](#)
- [\[EC2.170\] EC2 Startvorlagen sollten Instance Metadata Service Version 2 \(\) verwenden IMDSv2](#)
- [\[EC2.171\] Bei EC2 VPN-Verbindungen sollte die Protokollierung aktiviert sein](#)
- [\[EC2.172\] Die Einstellungen von EC2 VPC Block Public Access sollten den Internet-Gateway-Verkehr blockieren](#)

- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[EC2.174\] EC2 DHCP-Optionssätze sollten mit Tags versehen werden](#)
- [\[EC2.175\] EC2 Startvorlagen sollten mit Tags versehen sein](#)
- [\[EC2.176\] EC2 Präfixlisten sollten mit Tags versehen werden](#)
- [\[EC2.177\] EC2 Traffic Mirror-Sitzungen sollten mit Tags versehen werden](#)
- [\[EC2.178\] Filter für EC2 Verkehrsspiegel sollten mit Tags versehen werden](#)
- [\[EC2.179\] EC2 Traffic-Spiegel-Ziele sollten markiert werden](#)
- [\[EC2.180\] Bei EC2 Netzwerkschnittstellen sollte die source/destination Überprüfung aktiviert sein](#)
- [\[ECR.1\] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein](#)
- [\[ECR.2\] Bei privaten ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein](#)
- [\[ECR.3\] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein](#)
- [\[ECR.4\] Öffentliche ECR-Repositorys sollten markiert werden](#)
- [\[ECR.5\] ECR-Repositorys sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys](#)
- [\[ECS.1\] Amazon ECS-Aufgabendefinitionen sollten sichere Netzwerkmodi und Benutzerdefinitionen enthalten](#)
- [\[ECS.2\] ECS-Diensten sollten nicht automatisch öffentliche IP-Adressen zugewiesen werden](#)
- [\[ECS.3\] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen](#)
- [\[ECS.4\] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden](#)
- [\[ECS.5\] ECS-Container sollten auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sein](#)
- [\[ECS.8\] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden](#)
- [\[ECS.9\] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen](#)
- [\[ECS.10\] Die ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen](#)
- [\[ECS.12\] ECS-Cluster sollten Container Insights verwenden](#)
- [\[ECS.13\] ECS-Services sollten markiert werden](#)
- [\[ECS.14\] ECS-Cluster sollten markiert werden](#)
- [\[ECS.15\] ECS-Aufgabendefinitionen sollten mit Tags versehen werden](#)
- [\[ECS.16\] ECS-Aufgabensätze sollten öffentliche IP-Adressen nicht automatisch zuweisen](#)
- [\[ECS.17\] ECS-Aufgabendefinitionen sollten nicht den Host-Netzwerkmodus verwenden](#)

- [\[EFS.1\] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS](#)
- [\[EFS.2\] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein](#)
- [\[EFS.3\] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen](#)
- [\[EFS.4\] EFS-Zugangspunkte sollten eine Benutzeridentität erzwingen](#)
- [\[EFS.5\] EFS-Zugangspunkte sollten markiert werden](#)
- [\[EFS.6\] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden](#)
- [\[EFS.7\] Bei EFS-Dateisystemen sollten automatische Backups aktiviert sein](#)
- [\[EFS.8\] EFS-Dateisysteme sollten im Ruhezustand verschlüsselt werden](#)
- [\[EKS.1\] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein](#)
- [\[EKS.2\] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden](#)
- [\[EKS.3\] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden](#)
- [\[EKS.6\] EKS-Cluster sollten markiert werden](#)
- [\[EKS.7\] Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden](#)
- [\[EKS.8\] Bei EKS-Clustern sollte die Auditprotokollierung aktiviert sein](#)
- [\[ELB.2\] Classic Load Balancer mit SSL/HTTPS Listnern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager](#)
- [\[ELB.3\] Classic Load Balancer Balancer-Listener sollten mit HTTPS- oder TLS-Terminierung konfiguriert werden](#)
- [\[ELB.7\] Bei Classic Load Balancers sollte der Verbindungsabbau aktiviert sein](#)
- [\[ELB.8\] Classic Load Balancer mit SSL-Listnern sollten eine vordefinierte Sicherheitsrichtlinie mit starker Dauer verwenden AWS Config](#)
- [\[ELB.10\] Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken](#)
- [\[ELB.12\] Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden](#)
- [\[ELB.13\] Anwendungs-, Netzwerk- und Gateway-Load Balancer sollten sich über mehrere Availability Zones erstrecken](#)
- [\[ELB.14\] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden](#)
- [\[ELB.16\] Application Load Balancers sollten mit einer Web-ACL verknüpft sein AWS WAF](#)
- [\[ELB.17\] Anwendungs- und Netzwerk-Load-Balancer mit Listnern sollten die empfohlenen Sicherheitsrichtlinien verwenden](#)

- [\[ELB.18\] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln](#)
- [Bei \[ElastiCache.1\] ElastiCache \(Redis OSS\) -Clustern sollten automatische Backups aktiviert sein](#)
- [\[ElastiCache.2\] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein](#)
- [\[ElastiCache.3\] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein](#)
- [\[ElastiCache.4\] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden](#)
- [\[ElastiCache.5\] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden](#)
- [\[ElastiCache.6\] Für Replikationsgruppen ElastiCache \(Redis OSS\) früherer Versionen sollte Redis OSS AUTH aktiviert sein](#)
- [\[ElastiCache.7\] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden](#)
- [\[ElasticBeanstalk.1\] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben](#)
- [\[ElasticBeanstalk.2\] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk sollte Logs streamen nach CloudWatch](#)
- [\[EMR.1\] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben](#)
- [\[EMR.2\] Die Amazon EMR-Einstellung zum Blockieren des öffentlichen Zugriffs sollte aktiviert sein](#)
- [\[EMR.3\] Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden](#)
- [\[EMR.4\] Amazon EMR-Sicherheitskonfigurationen sollten bei der Übertragung verschlüsselt werden](#)
- [\[ES.1\] Bei Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein](#)
- [\[ES.2\] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein](#)
- [\[ES.3\] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden](#)
- [\[ES.4\] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein](#)
- [\[ES.5\] Für Elasticsearch-Domains sollte die Audit-Protokollierung aktiviert sein](#)
- [\[ES.6\] Elasticsearch-Domains sollten mindestens drei Datenknoten haben](#)
- [\[ES.7\] Elasticsearch-Domänen sollten mit mindestens drei dedizierten Master-Knoten konfiguriert werden](#)
- [\[ES.8\] Verbindungen zu Elasticsearch-Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden](#)
- [\[ES.9\] Elasticsearch-Domains sollten markiert werden](#)

- [\[EventBridge.2\] EventBridge Eventbusse sollten gekennzeichnet sein](#)
- [\[EventBridge.3\] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden](#)
- [\[EventBridge.4\] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[FSx.1\] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden](#)
- [\[FSx.2\] FSx für Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden](#)
- [\[FSx.3\] FSx für OpenZFS-Dateisysteme sollte für die Multi-AZ-Bereitstellung konfiguriert werden](#)
- [\[FSx.4\] FSx für NetApp ONTAP-Dateisysteme sollte für die Multi-AZ-Bereitstellung konfiguriert sein](#)
- [\[FSx.5\] FSx für Windows-Dateiserver sollten für die Multi-AZ-Bereitstellung konfiguriert sein](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[Glue.1\] AWS Glue Jobs sollten markiert werden](#)
- [\[Glue.3\] Transformationen für AWS Glue maschinelles Lernen sollten im Ruhezustand verschlüsselt werden](#)
- [\[Glue.4\] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue](#)
- [\[GuardDuty.1\] GuardDuty sollte aktiviert sein](#)
- [\[GuardDuty.2\] GuardDuty Filter sollten mit Tags versehen sein](#)
- [\[GuardDuty.3\] GuardDuty IPSets sollte markiert werden](#)
- [\[GuardDuty.4\] GuardDuty Detektoren sollten markiert werden](#)
- [\[GuardDuty.5\] GuardDuty EKS Audit Log Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.6\] GuardDuty Lambda Protection sollte aktiviert sein](#)
- [\[GuardDuty.7\] GuardDuty EKS Runtime Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.8\] Der GuardDuty Malware-Schutz für EC2 sollte aktiviert sein](#)
- [\[GuardDuty.9\] Der GuardDuty RDS-Schutz sollte aktiviert sein](#)
- [\[GuardDuty.10\] Der GuardDuty S3-Schutz sollte aktiviert sein](#)

- [\[GuardDuty.11\] GuardDuty Runtime Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.12\] GuardDuty ECS Runtime Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.13\] GuardDuty EC2 Runtime Monitoring sollte aktiviert sein](#)
- [\[IAM.1\] IAM-Richtlinien sollten keine vollen „*“-Administratorrechte zulassen](#)
- [\[IAM.2\] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein](#)
- [\[IAM.3\] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden](#)
- [\[IAM.4\] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren](#)
- [\[IAM.5\] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen](#)
- [\[IAM.6\] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.](#)
- [\[IAM.7\] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein](#)
- [\[IAM.8\] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden](#)
- [\[IAM.9\] MFA sollte für den Root-Benutzer aktiviert sein](#)
- [\[IAM.10\] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein](#)
- [\[IAM.11\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert](#)
- [\[IAM.12\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert](#)
- [\[IAM.13\] Stellen Sie sicher, dass für die IAM-Passwortrichtlinie mindestens ein Symbol erforderlich ist](#)
- [\[IAM.14\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert](#)
- [\[IAM.15\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert](#)
- [\[IAM.16\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert](#)
- [\[IAM.17\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft](#)
- [\[IAM.18\] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS -Support](#)
- [\[IAM.19\] MFA sollte für alle IAM-Benutzer aktiviert sein](#)
- [\[IAM.21\] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen](#)

- [\[IAM.22\] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden](#)
- [\[IAM.23\] IAM Access Analyzer-Analyzer sollten markiert werden](#)
- [\[IAM.24\] IAM-Rollen sollten mit Tags versehen werden](#)
- [\[IAM.25\] IAM-Benutzer sollten markiert werden](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[IAM.27\] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWS Cloud Shell FullAccess](#)
- [\[IAM.28\] Der externe Zugriffsanalysator für IAM Access Analyzer sollte aktiviert sein](#)
- [\[Inspector.1\] Das EC2 Scannen mit Amazon Inspector sollte aktiviert sein](#)
- [\[Inspector.2\] Das Amazon Inspector ECR-Scannen sollte aktiviert sein](#)
- [\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)
- [\[Inspector.4\] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein](#)
- [\[IoT.1\] AWS IoT Device Defender Sicherheitsprofile sollten markiert werden](#)
- [\[IoT.2\] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden](#)
- [\[IoT.3\] AWS IoT Core -Dimensionen sollten markiert werden](#)
- [\[IoT.4\] AWS IoT Core Autorisierer sollten markiert werden](#)
- [\[IoT.5\] AWS IoT Core Rollenalias sollten markiert werden](#)
- [\[IoT.6\] AWS IoT Core Richtlinien sollten markiert werden](#)
- [\[IoT Events .1\] AWS IoT-Events-Eingaben sollten markiert werden](#)
- [\[IoT Events .2\] AWS IoT-Ereignisdetektormodelle sollten markiert werden](#)
- [\[IoT Events .3\] Alarmmodelle für AWS IoT Events sollten markiert werden](#)
- [\[IoT Site Wise.1\] AWS SiteWise IoT-Asset-Modelle sollten markiert werden](#)
- [\[IoT Site Wise.2\] AWS SiteWise IoT-Dashboards sollten markiert werden](#)
- [\[IoT Site Wise.3\] AWS SiteWise IoT-Gateways sollten markiert werden](#)
- [\[IoT Site Wise.4\] AWS SiteWise IoT-Portale sollten markiert werden](#)
- [\[IoT Site Wise.5\] AWS SiteWise IoT-Projekte sollten markiert werden](#)
- [\[IoT Twin Maker.1\] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden](#)
- [\[IoT Twin Maker.2\] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden](#)
- [\[IoT Twin Maker.3\] AWS TwinMaker IoT-Szenen sollten markiert werden](#)
- [\[IoT Twin Maker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)

- [\[Io TWireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[Io TWireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)
- [\[Io TWireless .3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)
- [\[Keyspaces.1\] Amazon Keyspaces Keyspaces sollten mit Tags versehen sein](#)
- [\[Kinesis.1\] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden](#)
- [\[Kinesis.2\] Kinesis-Streams sollten markiert werden](#)
- [\[Kinesis.3\] Kinesis-Streams sollten über eine angemessene Aufbewahrungsfrist für Daten verfügen](#)
- [\[KMS.1\] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)
- [\[KMS.2\] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)
- [\[KMS.3\] AWS KMS keys sollte nicht unbeabsichtigt gelöscht werden](#)
- [\[KMS.5\] KMS-Schlüssel sollten nicht öffentlich zugänglich sein](#)
- [\[Lambda.5\] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren](#)
- [\[Lambda.6\] Lambda-Funktionen sollten markiert werden](#)
- [\[Lambda.7\] Bei Lambda-Funktionen sollte aktives Tracing aktiviert sein AWS X-Ray](#)
- [\[Macie.1\] Amazon Macie sollte aktiviert sein](#)
- [\[Macie.2\] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein](#)
- [\[MQ.2\] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch](#)
- [\[MQ.3\] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein](#)
- [\[MQ.4\] Amazon MQ-Broker sollten markiert werden](#)
- [\[MQ.5\] ActiveMQ-Broker sollten den Aktiv-/Standby-Bereitstellungsmodus verwenden](#)
- [\[MQ.6\] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden](#)
- [\[MSK.1\] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden](#)
- [\[MSK.2\] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein](#)
- [\[MSK.3\] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden](#)
- [\[MSK.4\] Bei MSK-Clustern sollte der öffentliche Zugriff deaktiviert sein](#)

- [\[MSK.5\] Bei MSK-Konnektoren sollte die Protokollierung aktiviert sein](#)
- [\[MSK.6\] MSK-Cluster sollten den nicht authentifizierten Zugriff deaktivieren](#)
- [\[Neptune.1\] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.2\] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)
- [\[Neptune.3\] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein](#)
- [\[Neptune.4\] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[Neptune.5\] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein](#)
- [\[Neptune.6\] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.7\] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein](#)
- [\[Neptune.8\] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren](#)
- [\[Neptune.9\] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden](#)
- [\[NetworkFirewall.1\] Network firewalls sollten über mehrere Availability Zones hinweg bereitgestellt werden](#)
- [\[NetworkFirewall.2\] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein](#)
- [\[NetworkFirewall.3\] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet haben](#)
- [\[NetworkFirewall.4\] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ sein.](#)
- [\[NetworkFirewall.5\] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ sein.](#)
- [\[NetworkFirewall.6\] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein](#)
- [\[NetworkFirewall.7\] Netzwerk-Firewall-Firewalls sollten markiert werden](#)
- [\[NetworkFirewall.8\] Firewall-Richtlinien für Netzwerk-Firewalls sollten markiert werden](#)
- [\[NetworkFirewall.9\] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein](#)
- [\[NetworkFirewall.10\] Bei Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein](#)
- [Bei \[Opensearch.1\] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein](#)
- [\[Opensearch.2\] OpenSearch -Domains sollten nicht öffentlich zugänglich sein](#)
- [\[Opensearch.3\] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden](#)

- [Die Protokollierung von \[Opensearch.4\] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein](#)
- [Für \[Opensearch.5\] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein](#)
- [\[Opensearch.6\] OpenSearch Domains sollten mindestens drei Datenknoten haben](#)
- [Für \[Opensearch.7\] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein](#)
- [\[Opensearch.8\] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden](#)
- [\[Opensearch.9\] OpenSearch -Domains sollten mit Tags versehen werden](#)
- [Auf \[Opensearch.10\] OpenSearch -Domains sollte das neueste Softwareupdate installiert sein](#)
- [\[Opensearch.11\] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben](#)
- [\[PCA.1\] AWS Private CA Root-Zertifizierungsstelle sollte deaktiviert sein](#)
- [\[PCA.2\] AWS Private CA-Zertifizierungsstellen sollten gekennzeichnet werden](#)
- [\[RDS.14\] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein](#)
- [\[RDS.16\] Aurora-DB-Cluster sollten so konfiguriert sein, dass sie Tags in DB-Snapshots kopieren](#)
- [\[RDS.17\] RDS-DB-Instances sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren](#)
- [\[RDS.18\] RDS-Instances sollten in einer VPC bereitgestellt werden](#)
- [\[RDS.19\] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Cluster-Ereignisse konfiguriert werden](#)
- [\[RDS.20\] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Ereignisse der Datenbankinstanz konfiguriert werden](#)
- [\[RDS.21\] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbankparametergruppenereignisse konfiguriert werden](#)
- [\[RDS.22\] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbanksicherheitsgruppenereignisse konfiguriert werden](#)
- [\[RDS.23\] RDS-Instances sollten keinen Standard-Port für die Datenbank-Engine verwenden](#)
- [\[RDS.24\] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden](#)
- [\[RDS.25\] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden](#)
- [\[RDS.26\] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden](#)
- [\[RDS.27\] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[RDS.28\] RDS-DB-Cluster sollten markiert werden](#)

- [\[RDS.29\] RDS-DB-Cluster-Snapshots sollten markiert werden](#)
- [\[RDS.30\] RDS-DB-Instances sollten markiert werden](#)
- [\[RDS.31\] RDS-DB-Sicherheitsgruppen sollten markiert werden](#)
- [\[RDS.32\] RDS-DB-Snapshots sollten markiert werden](#)
- [\[RDS.33\] RDS-DB-Subnetzgruppen sollten markiert werden](#)
- [\[RDS.34\] Aurora MySQL-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)
- [\[RDS.35\] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein](#)
- [\[RDS.36\] RDS für PostgreSQL-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[RDS.37\] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[RDS.38\] RDS für PostgreSQL-DB-Instances sollten bei der Übertragung verschlüsselt werden](#)
- [\[RDS.39\] RDS für MySQL-DB-Instances sollten bei der Übertragung verschlüsselt werden](#)
- [\[RDS.40\] RDS für SQL Server-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[RDS.41\] RDS für SQL Server-DB-Instances sollten bei der Übertragung verschlüsselt werden](#)
- [\[RDS.42\] RDS für MariaDB-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[RDS.44\] RDS für MariaDB-DB-Instances sollte bei der Übertragung verschlüsselt werden](#)
- [\[RDS.45\] Bei Aurora MySQL-DB-Clustern sollte die Audit-Protokollierung aktiviert sein](#)
- [\[Redshift.1\] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten](#)
- [\[Redshift.2\] Verbindungen zu Amazon Redshift Redshift-Clustern sollten bei der Übertragung verschlüsselt werden](#)
- [\[Redshift.3\] Bei Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein](#)
- [\[Redshift.4\] Bei Amazon Redshift Redshift-Clustern sollte die Auditprotokollierung aktiviert sein](#)
- [\[Redshift.6\] Bei Amazon Redshift sollten automatische Upgrades auf Hauptversionen aktiviert sein](#)
- [\[Redshift.7\] Redshift-Cluster sollten erweitertes VPC-Routing verwenden](#)
- [\[Redshift.8\] Amazon Redshift Redshift-Cluster sollten nicht den standardmäßigen Admin-Benutzernamen verwenden](#)
- [\[Redshift.9\] Redshift-Cluster sollten nicht den Standard-Datenbanknamen verwenden](#)
- [\[Redshift.10\] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[Redshift.11\] Redshift-Cluster sollten markiert werden](#)
- [\[Redshift.12\] Abonnements für Redshift-Ereignisbenachrichtigungen sollten markiert werden](#)
- [\[Redshift.13\] Redshift-Cluster-Snapshots sollten markiert werden](#)

- [\[Redshift.14\] Redshift-Cluster-Subnetzgruppen sollten markiert werden](#)
- [\[Redshift.15\] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen](#)
- [\[Redshift.16\] Redshift-Cluster-Subnetzgruppen sollten Subnetze aus mehreren Availability Zones haben](#)
- [\[Redshift.17\] Redshift-Cluster-Parametergruppen sollten markiert werden](#)
- [\[Redshift.18\] Für Redshift-Cluster sollten Multi-AZ-Bereitstellungen aktiviert sein](#)
- [\[RedshiftServerless.1\] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden](#)
- [\[RedshiftServerless.2\] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein](#)
- [\[RedshiftServerless.3\] Serverlose Redshift-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten](#)
- [\[RedshiftServerless.4\] Serverlose Redshift-Namespaces sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys](#)
- [\[RedshiftServerless.5\] Redshift Serverless-Namespaces sollten nicht den Standard-Admin-Benutzernamen verwenden](#)
- [\[RedshiftServerless.6\] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch](#)
- [\[RedshiftServerless.7\] Redshift Serverless-Namespaces sollten nicht den Standard-Datenbanknamen verwenden](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.7\] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden](#)
- [\[S3.10\] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben](#)
- [\[S3.11\] Bei S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein](#)
- [\[S3.12\] ACLs sollte nicht zur Verwaltung des Benutzerzugriffs auf S3-Allzweck-Buckets verwendet werden](#)
- [\[S3.13\] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben](#)
- [\[S3.17\] S3-Allzweck-Buckets sollten im Ruhezustand verschlüsselt werden mit AWS KMS keys](#)
- [\[S3.19\] Bei S3-Zugriffspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.20\] Bei S3-Allzweck-Buckets sollte MFA Delete aktiviert sein](#)

- [\[S3.22\] S3-Allzweck-Buckets sollten Schreibereignisse auf Objektebene protokollieren](#)
- [\[S3.23\] S3-Allzweck-Buckets sollten Leseereignisse auf Objektebene protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)
- [\[SageMaker.1\] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben](#)
- [\[SageMaker.2\] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden](#)
- [\[SageMaker.3\] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben](#)
- [\[SageMaker.4\] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein](#)
- [\[SageMaker.5\] SageMaker Modelle sollten eingehenden Datenverkehr blockieren](#)
- [\[SageMaker.6\] SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden](#)
- [\[SageMaker.7\] SageMaker Bilder sollten mit Tags versehen werden](#)
- [\[SageMaker.8\] SageMaker Notebook-Instances sollten auf unterstützten Plattformen laufen](#)
- [\[SES.1\] SES-Kontaktlisten sollten mit Tags versehen werden](#)
- [\[SES.2\] SES-Konfigurationssätze sollten mit Tags versehen werden](#)
- [\[SecretsManager.1\] Bei Secrets Manager Manager-Geheimnissen sollte die automatische Rotation aktiviert sein](#)
- [\[SecretsManager.2\] Secrets Manager Manager-Geheimnisse, die mit automatischer Rotation konfiguriert sind, sollten erfolgreich rotieren](#)
- [\[SecretsManager.3\] Unbenutzte Secrets Manager Manager-Geheimnisse entfernen](#)
- [\[SecretsManager.4\] Secrets Manager Manager-Geheimnisse sollten innerhalb einer bestimmten Anzahl von Tagen rotiert werden](#)
- [\[SecretsManager.5\] Secrets Manager Manager-Geheimnisse sollten markiert werden](#)
- [\[ServiceCatalog.1\] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden](#)
- [\[SNS.3\] SNS-Themen sollten markiert werden](#)
- [\[SNS.4\] Zugriffsrichtlinien für SNS-Themen sollten keinen öffentlichen Zugriff zulassen](#)
- [\[SQS.1\] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt werden](#)
- [\[SQS.2\] SQS-Warteschlangen sollten markiert werden](#)

- [\[SQS.3\] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen](#)
- [\[SSM.1\] EC2 Amazon-Instances sollten verwaltet werden von AWS Systems Manager](#)
- [\[SSM.2\] Von Systems Manager verwaltete EC2 Amazon-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben](#)
- [\[SSM.3\] Von Systems Manager verwaltete EC2 Amazon-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben](#)
- [\[SSM.4\] SSM-Dokumente sollten nicht öffentlich sein](#)
- [\[SSM.5\] SSM-Dokumente sollten mit Tags versehen werden](#)
- [\[SSM.6\] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[SSM.7\] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein](#)
- [\[StepFunctions.1\] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben](#)
- [\[StepFunctions.2\] Die Aktivitäten von Step Functions sollten mit Tags versehen werden](#)
- [\[Transfer.1\] AWS Transfer Family -Workflows sollten mit Tags versehen werden](#)
- [\[Transfer.2\] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden](#)
- [\[Transfer.3\] Bei Connectoren der Transfer-Familie sollte die Protokollierung aktiviert sein](#)
- [\[Transfer.4\] Transfer Family Familienverträge sollten gekennzeichnet werden](#)
- [\[Transfer.5\] Transfer Family Familienzertifikate sollten gekennzeichnet sein](#)
- [\[Transfer.6\] Steckverbinder der Transfer-Familie sollten gekennzeichnet sein](#)
- [\[Transfer.7\] Familienprofile sollten mit Tags versehen werden](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.2\] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.3\] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.4\] AWS WAF Classic Regional Web ACLs sollte mindestens eine Regel oder Regelgruppe enthalten](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)

- [\[WAF.10\] AWS WAF web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WAF.11\] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein](#)
- [Für \[WAF.12\] AWS WAF Regeln sollten Metriken aktiviert sein CloudWatch](#)
- [\[WorkSpaces.1\] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden](#)
- [\[WorkSpaces.2\] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden](#)

Asien-Pazifik (Thailand)

Die folgenden Steuerelemente werden in der Region Asien-Pazifik (Thailand) nicht unterstützt.

- [\[ACM.1\] Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden](#)
- [\[ACM.2\] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden](#)
- [\[ACM.3\] ACM-Zertifikate sollten mit einem Tag versehen werden](#)
- [\[Account.1\] Sicherheitskontakthinformationen sollten bereitgestellt werden für AWS-Konto](#)
- [\[Account.2\] AWS-Konten sollte Teil einer Organisation sein AWS Organizations](#)
- [\[APIGateway.1\] API Gateway REST und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein](#)
- [\[APIGateway.5\] API Gateway REST API-Cache-Daten sollten im Ruhezustand verschlüsselt werden](#)
- [\[APIGateway.8\] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben](#)
- [\[APIGateway.9\] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein](#)
- [\[Amplify.1\] Amplify-Apps sollten markiert werden](#)
- [\[Amplify.2\] Amplify-Zweige sollten markiert werden](#)
- [\[AppConfig.1\] AWS AppConfig Anwendungen sollten markiert werden](#)
- [\[AppConfig.2\] AWS AppConfig Konfigurationsprofile sollten mit Tags versehen werden](#)
- [\[AppConfig.3\] AWS AppConfig Umgebungen sollten markiert werden](#)
- [\[AppConfig.4\] AWS AppConfig Erweiterungszuordnungen sollten markiert werden](#)
- [\[AppFlow.1\] AppFlow Amazon-Datenflüsse sollten mit Tags versehen werden](#)
- [\[AppRunner.1\] App Runner-Dienste sollten markiert sein](#)
- [\[AppRunner.2\] App Runner VPC-Konnektoren sollten markiert sein](#)

- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.2\] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben](#)
- [\[AppSync.4\] AWS AppSync GraphQL APIs sollte markiert sein](#)
- [\[AppSync.5\] AWS AppSync GraphQL APIs sollte nicht mit API-Schlüsseln authentifiziert werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [\[Athena.2\] Athena-Datenkataloge sollten mit Tags versehen werden](#)
- [\[Athena.3\] Athena-Arbeitsgruppen sollten markiert werden](#)
- [\[Athena.4\] Bei Athena-Arbeitsgruppen sollte die Protokollierung aktiviert sein](#)
- [\[AutoScaling.2\] Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken](#)
- [\[AutoScaling.3\] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2 Instances so konfigurieren, dass sie Instance Metadata Service Version 2 \(IMDSv2\) benötigen](#)
- [\[AutoScaling.6\] Auto Scaling Scaling-Gruppen sollten mehrere Instance-Typen in mehreren Availability Zones verwenden](#)
- [\[AutoScaling.9\] Amazon EC2 Auto Scaling Scaling-Gruppen sollten EC2 Amazon-Startvorlagen verwenden](#)
- [\[AutoScaling.10\] EC2 Auto Scaling Scaling-Gruppen sollten markiert werden](#)
- [\[Backup.1\] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein](#)
- [\[Backup.2\] AWS Backup Wiederherstellungspunkte sollten markiert werden](#)
- [\[Backup.3\] AWS Backup Tresore sollten markiert sein](#)
- [\[Backup.4\] AWS Backup Berichtspläne sollten markiert werden](#)
- [\[Backup.5\] AWS Backup Backup-Pläne sollten markiert werden](#)
- [\[Batch.1\] Warteschlangen für Batch-Jobs sollten markiert werden](#)
- [\[Batch.2\] Richtlinien für die Batch-Planung sollten gekennzeichnet sein](#)
- [\[Batch.3\] Batch-Computing-Umgebungen sollten markiert werden](#)
- [\[Batch.4\] Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden](#)
- [\[CloudFormation.2\] CloudFormation Stapel sollten markiert werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)

- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[CloudTrail.6\] Sicherstellen, dass der S3-Bucket, in dem CloudTrail Protokolle gespeichert werden, nicht öffentlich zugänglich ist](#)
- [\[CloudTrail.7\] Sicherstellen, dass die S3-Bucket-Zugriffsprotokollierung für den CloudTrail S3-Bucket aktiviert ist](#)
- [\[CloudTrail.9\] CloudTrail Pfade sollten markiert werden](#)
- [\[CloudTrail.10\] Event-Datenspeicher in CloudTrail Lake sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys](#)
- [\[CloudWatch.17\] CloudWatch Alarmaktionen sollten aktiviert sein](#)
- [\[CodeArtifact.1\] CodeArtifact Repositorien sollten mit Tags versehen werden](#)
- [\[CodeBuild.1\] Das CodeBuild Bitbucket-Quell-Repository URLs sollte keine vertraulichen Anmeldeinformationen enthalten](#)
- [\[CodeBuild.2\] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten](#)
- [\[CodeBuild.3\] CodeBuild S3-Protokolle sollten verschlüsselt sein](#)
- [\[CodeBuild.4\] CodeBuild Projektumgebungen sollten eine AWS Config Protokollierungsdauer haben](#)

- [\[CodeBuild.7\] Exporte von CodeBuild Berichtsgruppen sollten im Ruhezustand verschlüsselt werden](#)
- [\[CodeGuruProfiler.1\] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden](#)
- [\[CodeGuruReviewer.1\] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden](#)
- [\[Cognito.1\] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein](#)
- [\[Cognito.2\] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen](#)
- [\[Connect.1\] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden](#)
- [\[Connect.2\] Für Amazon Connect Connect-Instances sollte die Protokollierung aktiviert sein](#)
[CloudWatch](#)
- [\[DataFirehose.1\] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden](#)
- [\[DataSync.1\] Für DataSync Aufgaben sollte die Protokollierung aktiviert sein](#)
- [\[DataSync.2\] DataSync Aufgaben sollten mit Tags versehen werden](#)
- [\[Detective.1\] Verhaltensdiagramme von Detektiven sollten markiert werden](#)
- [\[DMS.1\] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein](#)
- [\[DMS.2\] DMS-Zertifikate sollten gekennzeichnet sein](#)
- [\[DMS.3\] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden](#)
- [\[DMS.4\] DMS-Replikationsinstanzen sollten markiert werden](#)
- [\[DMS.5\] Subnetzgruppen für die DMS-Replikation sollten markiert werden](#)
- [\[DMS.6\] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein](#)
- [\[DMS.7\] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.8\] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.9\] DMS-Endpunkte sollten SSL verwenden](#)
- [\[DMS.10\] Bei DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein](#)
- [\[DMS.11\] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein](#)
- [\[DMS.12\] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein](#)
- [\[DocumentDB.1\] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden](#)

- [\[DocumentDB.2\] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen](#)
- [\[DocumentDB.3\] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein](#)
- [\[DocumentDB.4\] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch](#)
- [\[DocumentDB.5\] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[DocumentDB.6\] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[DynamoDB.3\] DynamoDB Accelerator \(DAX\) -Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DynamoDB.4\] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein](#)
- [\[DynamoDB.5\] DynamoDB-Tabellen sollten mit Tags versehen werden](#)
- [\[DynamoDB.6\] Bei DynamoDB-Tabellen sollte der Löschschutz aktiviert sein](#)
- [\[DynamoDB.7\] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[EC2.4\] Gestoppte EC2 Instances sollten nach einem bestimmten Zeitraum entfernt werden](#)
- [\[EC2.21\] Das Netzwerk ACLs sollte keinen Zugang von 0.0.0.0/0 zu Port 22 oder Port 3389 zulassen](#)
- [\[EC2.22\] Ungenutzte EC2 Amazon-Sicherheitsgruppen sollten entfernt werden](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways sollte VPC-Anhangsanfragen nicht automatisch akzeptieren](#)
- [\[EC2.24\] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden](#)
- [\[EC2.25\] EC2 Amazon-Startvorlagen sollten Netzwerkschnittstellen nicht öffentlich IPs zuweisen](#)
- [\[EC2.28\] EBS-Volumes sollten durch einen Backup-Plan abgedeckt sein](#)
- [\[EC2.33\] EC2 Transit-Gateway-Anhänge sollten mit Tags versehen werden](#)
- [\[EC2.34\] Die Routentabellen für EC2 Transit-Gateways sollten mit Tags versehen werden](#)
- [\[EC2.35\] EC2 Netzwerkschnittstellen sollten markiert werden](#)
- [\[EC2.36\] EC2 Kunden-Gateways sollten mit Tags versehen werden](#)
- [\[EC2.37\] EC2 Elastische IP-Adressen sollten mit Tags versehen werden](#)
- [\[EC2.38\] EC2 Instances sollten markiert werden](#)
- [\[EC2.39\] EC2 Internet-Gateways sollten markiert werden](#)
- [\[EC2.40\] EC2 NAT-Gateways sollten markiert werden](#)

- [\[EC2.41\] Das EC2 Netzwerk ACLs sollte markiert sein](#)
- [\[EC2.42\] EC2 Routing-Tabellen sollten mit Tags versehen werden](#)
- [\[EC2.43\] EC2 Sicherheitsgruppen sollten markiert werden](#)
- [\[EC2.44\] EC2 Subnetze sollten markiert werden](#)
- [\[EC2.45\] EC2 Volumen sollten mit Tags versehen werden](#)
- [\[EC2.46\] Amazon VPCs sollte markiert werden](#)
- [\[EC2.47\] Amazon VPC Endpoint Services sollten markiert werden](#)
- [\[EC2.48\] Amazon VPC-Flow-Logs sollten mit Tags versehen werden](#)
- [\[EC2.49\] Amazon VPC-Peering-Verbindungen sollten markiert werden](#)
- [\[EC2.50\] EC2 VPN-Gateways sollten markiert werden](#)
- [\[EC2.51\] EC2 Client-VPN-Endpunkte sollten die Client-Verbindungsprotokollierung aktiviert haben](#)
- [\[EC2.52\] EC2 Transit-Gateways sollten markiert werden](#)
- [\[EC2.53\] EC2 Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 zu Remote-Serververwaltungsports zulassen](#)
- [\[EC2.54\] EC2 Sicherheitsgruppen sollten keinen Zugriff von: :/0 zu Remote-Serveradministrationsports zulassen](#)
- [\[EC2.55\] VPCs sollte mit einem Schnittstellenendpunkt für die ECR-API konfiguriert werden](#)
- [\[EC2.56\] VPCs sollte mit einem Schnittstellenendpunkt für Docker Registry konfiguriert werden](#)
- [\[EC2.57\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager konfiguriert werden](#)
- [\[EC2.58\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert sein](#)
- [\[EC2.60\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden](#)
- [\[EC2.170\] EC2 Startvorlagen sollten Instance Metadata Service Version 2 \(\) verwenden IMDSv2](#)
- [\[EC2.171\] Bei EC2 VPN-Verbindungen sollte die Protokollierung aktiviert sein](#)
- [\[EC2.172\] Die Einstellungen von EC2 VPC Block Public Access sollten den Internet-Gateway-Verkehr blockieren](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[EC2.174\] EC2 DHCP-Optionssätze sollten mit Tags versehen werden](#)
- [\[EC2.175\] EC2 Startvorlagen sollten mit Tags versehen sein](#)

- [\[EC2.176\] EC2 Präfixlisten sollten mit Tags versehen werden](#)
- [\[EC2.177\] EC2 Traffic Mirror-Sitzungen sollten mit Tags versehen werden](#)
- [\[EC2.178\] Filter für EC2 Verkehrsspiegel sollten mit Tags versehen werden](#)
- [\[EC2.179\] EC2 Traffic-Spiegel-Ziele sollten markiert werden](#)
- [\[EC2.180\] Bei EC2 Netzwerkschnittstellen sollte die source/destination Überprüfung aktiviert sein](#)
- [\[ECR.1\] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein](#)
- [\[ECR.2\] Bei privaten ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein](#)
- [\[ECR.3\] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein](#)
- [\[ECR.4\] Öffentliche ECR-Repositorien sollten markiert werden](#)
- [\[ECR.5\] ECR-Repositorys sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys](#)
- [\[ECS.2\] ECS-Diensten sollten nicht automatisch öffentliche IP-Adressen zugewiesen werden](#)
- [\[ECS.3\] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen](#)
- [\[ECS.4\] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden](#)
- [\[ECS.5\] ECS-Container sollten auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sein](#)
- [\[ECS.8\] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden](#)
- [\[ECS.9\] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen](#)
- [\[ECS.10\] Die ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen](#)
- [\[ECS.12\] ECS-Cluster sollten Container Insights verwenden](#)
- [\[ECS.13\] ECS-Services sollten markiert werden](#)
- [\[ECS.14\] ECS-Cluster sollten markiert werden](#)
- [\[ECS.15\] ECS-Aufgabendefinitionen sollten mit Tags versehen werden](#)
- [\[ECS.16\] ECS-Aufgabensätze sollten öffentliche IP-Adressen nicht automatisch zuweisen](#)
- [\[ECS.17\] ECS-Aufgabendefinitionen sollten nicht den Host-Netzwerkmodus verwenden](#)
- [\[EFS.1\] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS](#)
- [\[EFS.2\] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein](#)
- [\[EFS.3\] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen](#)
- [\[EFS.4\] EFS-Zugangspunkte sollten eine Benutzeridentität erzwingen](#)

- [\[EFS.5\] EFS-Zugangspunkte sollten markiert werden](#)
- [\[EFS.6\] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden](#)
- [\[EFS.7\] Bei EFS-Dateisystemen sollten automatische Backups aktiviert sein](#)
- [\[EFS.8\] EFS-Dateisysteme sollten im Ruhezustand verschlüsselt werden](#)
- [\[EKS.2\] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden](#)
- [\[EKS.3\] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden](#)
- [\[EKS.6\] EKS-Cluster sollten markiert werden](#)
- [\[EKS.7\] Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden](#)
- [\[EKS.8\] Bei EKS-Clustern sollte die Auditprotokollierung aktiviert sein](#)
- [\[ELB.7\] Bei Classic Load Balancern sollte der Verbindungsabbau aktiviert sein](#)
- [\[ELB.10\] Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken](#)
- [\[ELB.12\] Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden](#)
- [\[ELB.13\] Anwendungs-, Netzwerk- und Gateway-Load Balancer sollten sich über mehrere Availability Zones erstrecken](#)
- [\[ELB.14\] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden](#)
- [\[ELB.17\] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden](#)
- [\[ELB.18\] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln](#)
- [Bei \[ElastiCache.1\] ElastiCache \(Redis OSS\) -Clustern sollten automatische Backups aktiviert sein](#)
- [\[ElastiCache.2\] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein](#)
- [\[ElastiCache.3\] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein](#)
- [\[ElastiCache.4\] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden](#)
- [\[ElastiCache.5\] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden](#)
- [\[ElastiCache.6\] Für Replikationsgruppen ElastiCache \(Redis OSS\) früherer Versionen sollte Redis OSS AUTH aktiviert sein](#)
- [\[ElastiCache.7\] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden](#)
- [\[ElasticBeanstalk.1\] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben](#)

- [\[ElasticBeanstalk.2\] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk sollte Logs streamen nach CloudWatch](#)
- [\[EMR.1\] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben](#)
- [\[EMR.2\] Die Amazon EMR-Einstellung zum Blockieren des öffentlichen Zugriffs sollte aktiviert sein](#)
- [\[EMR.3\] Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden](#)
- [\[EMR.4\] Amazon EMR-Sicherheitskonfigurationen sollten bei der Übertragung verschlüsselt werden](#)
- [\[ES.3\] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden](#)
- [\[ES.4\] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein](#)
- [\[ES.5\] Für Elasticsearch-Domains sollte die Audit-Protokollierung aktiviert sein](#)
- [\[ES.6\] Elasticsearch-Domains sollten mindestens drei Datenknoten haben](#)
- [\[ES.7\] Elasticsearch-Domänen sollten mit mindestens drei dedizierten Master-Knoten konfiguriert werden](#)
- [\[ES.8\] Verbindungen zu Elasticsearch-Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden](#)
- [\[ES.9\] Elasticsearch-Domains sollten markiert werden](#)
- [\[EventBridge.2\] EventBridge Eventbusse sollten gekennzeichnet sein](#)
- [\[EventBridge.3\] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden](#)
- [\[EventBridge.4\] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[FSx.1\] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden](#)
- [\[FSx.2\] FSx für Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden](#)
- [\[FSx.3\] FSx für OpenZFS-Dateisysteme sollte für die Multi-AZ-Bereitstellung konfiguriert werden](#)
- [\[FSx.4\] FSx für NetApp ONTAP-Dateisysteme sollte für die Multi-AZ-Bereitstellung konfiguriert sein](#)
- [\[FSx.5\] FSx für Windows-Dateiserver sollten für die Multi-AZ-Bereitstellung konfiguriert sein](#)

- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[Glue.1\] AWS Glue Jobs sollten markiert werden](#)
- [\[Glue.3\] Transformationen für AWS Glue maschinelles Lernen sollten im Ruhezustand verschlüsselt werden](#)
- [\[Glue.4\] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue](#)
- [\[GuardDuty.1\] GuardDuty sollte aktiviert sein](#)
- [\[GuardDuty.2\] GuardDuty Filter sollten mit Tags versehen sein](#)
- [\[GuardDuty.3\] GuardDuty IPSets sollte markiert werden](#)
- [\[GuardDuty.4\] GuardDuty Detektoren sollten markiert werden](#)
- [\[GuardDuty.5\] GuardDuty EKS Audit Log Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.6\] GuardDuty Lambda Protection sollte aktiviert sein](#)
- [\[GuardDuty.7\] GuardDuty EKS Runtime Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.8\] Der GuardDuty Malware-Schutz für EC2 sollte aktiviert sein](#)
- [\[GuardDuty.9\] Der GuardDuty RDS-Schutz sollte aktiviert sein](#)
- [\[GuardDuty.10\] Der GuardDuty S3-Schutz sollte aktiviert sein](#)
- [\[GuardDuty.11\] GuardDuty Runtime Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.12\] GuardDuty ECS Runtime Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.13\] GuardDuty EC2 Runtime Monitoring sollte aktiviert sein](#)
- [\[IAM.1\] IAM-Richtlinien sollten keine vollen „*“-Administratorrechte zulassen](#)
- [\[IAM.2\] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein](#)
- [\[IAM.3\] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden](#)
- [\[IAM.4\] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren](#)
- [\[IAM.5\] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen](#)
- [\[IAM.6\] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.](#)
- [\[IAM.7\] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein](#)
- [\[IAM.8\] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden](#)
- [\[IAM.9\] MFA sollte für den Root-Benutzer aktiviert sein](#)
- [\[IAM.10\] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein](#)

- [\[IAM.11\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert](#)
- [\[IAM.12\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert](#)
- [\[IAM.13\] Stellen Sie sicher, dass für die IAM-Passwortrichtlinie mindestens ein Symbol erforderlich ist](#)
- [\[IAM.14\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert](#)
- [\[IAM.15\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert](#)
- [\[IAM.16\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert](#)
- [\[IAM.17\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft](#)
- [\[IAM.18\] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS -Support](#)
- [\[IAM.19\] MFA sollte für alle IAM-Benutzer aktiviert sein](#)
- [\[IAM.21\] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen](#)
- [\[IAM.22\] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden](#)
- [\[IAM.23\] IAM Access Analyzer-Analyzer sollten markiert werden](#)
- [\[IAM.24\] IAM-Rollen sollten mit Tags versehen werden](#)
- [\[IAM.25\] IAM-Benutzer sollten markiert werden](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[IAM.27\] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWS Cloud Shell Full Access](#)
- [\[IAM.28\] Der externe Zugriffsanalysator für IAM Access Analyzer sollte aktiviert sein](#)
- [\[Inspector.1\] Das EC2 Scannen mit Amazon Inspector sollte aktiviert sein](#)
- [\[Inspector.2\] Das Amazon Inspector ECR-Scannen sollte aktiviert sein](#)
- [\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)
- [\[Inspector.4\] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein](#)
- [\[IoT.1\] AWS IoT Device Defender Sicherheitsprofile sollten markiert werden](#)
- [\[IoT.2\] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden](#)

- [\[IoT.3\] AWS IoT Core -Dimensionen sollten markiert werden](#)
- [\[IoT.4\] AWS IoT Core Autorisierer sollten markiert werden](#)
- [\[IoT.5\] AWS IoT Core Rollenalias sollten markiert werden](#)
- [\[IoT.6\] AWS IoT Core Richtlinien sollten markiert werden](#)
- [\[IoTEvents .1\] AWS IoT-Events-Eingaben sollten markiert werden](#)
- [\[IoTEvents .2\] AWS IoT-Ereignisdetektormodelle sollten markiert werden](#)
- [\[IoTEvents .3\] Alarmmodelle für AWS IoT Events sollten markiert werden](#)
- [\[IoTSiteWise.1\] AWS SiteWise IoT-Asset-Modelle sollten markiert werden](#)
- [\[IoTSiteWise.2\] AWS SiteWise IoT-Dashboards sollten markiert werden](#)
- [\[IoTSiteWise.3\] AWS SiteWise IoT-Gateways sollten markiert werden](#)
- [\[IoTSiteWise.4\] AWS SiteWise IoT-Portale sollten markiert werden](#)
- [\[IoTSiteWise.5\] AWS SiteWise IoT-Projekte sollten markiert werden](#)
- [\[IoT Twin Maker.1\] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden](#)
- [\[IoT Twin Maker.2\] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden](#)
- [\[IoT Twin Maker.3\] AWS TwinMaker IoT-Szenen sollten markiert werden](#)
- [\[IoT Twin Maker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[IoTWireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[IoTWireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)
- [\[IoTWireless .3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)
- [\[Keyspaces.1\] Amazon Keyspaces Keyspaces sollten mit Tags versehen sein](#)
- [\[Kinesis.1\] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden](#)
- [\[Kinesis.2\] Kinesis-Streams sollten markiert werden](#)
- [\[Kinesis.3\] Kinesis-Streams sollten über eine angemessene Aufbewahrungsfrist für Daten verfügen](#)
- [\[KMS.1\] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)
- [\[KMS.2\] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)

- [\[KMS.3\] AWS KMS keys sollte nicht unbeabsichtigt gelöscht werden](#)
- [\[KMS.5\] KMS-Schlüssel sollten nicht öffentlich zugänglich sein](#)
- [\[Lambda.5\] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren](#)
- [\[Lambda.6\] Lambda-Funktionen sollten markiert werden](#)
- [\[Lambda.7\] Bei Lambda-Funktionen sollte aktives Tracing aktiviert sein AWS X-Ray](#)
- [\[Macie.1\] Amazon Macie sollte aktiviert sein](#)
- [\[Macie.2\] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein](#)
- [\[MQ.2\] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch](#)
- [\[MQ.3\] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein](#)
- [\[MQ.4\] Amazon MQ-Broker sollten markiert werden](#)
- [\[MQ.5\] ActiveMQ-Broker sollten den Aktiv-/Standby-Bereitstellungsmodus verwenden](#)
- [\[MQ.6\] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden](#)
- [\[MSK.1\] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden](#)
- [\[MSK.2\] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein](#)
- [\[MSK.3\] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden](#)
- [\[MSK.4\] Bei MSK-Clustern sollte der öffentliche Zugriff deaktiviert sein](#)
- [\[MSK.5\] Bei MSK-Konnektoren sollte die Protokollierung aktiviert sein](#)
- [\[MSK.6\] MSK-Cluster sollten den nicht authentifizierten Zugriff deaktivieren](#)
- [\[Neptune.1\] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.2\] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)
- [\[Neptune.3\] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein](#)
- [\[Neptune.4\] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[Neptune.5\] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein](#)
- [\[Neptune.6\] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.7\] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein](#)
- [\[Neptune.8\] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren](#)
- [\[Neptune.9\] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden](#)
- [\[NetworkFirewall.1\] Network firewalls sollten über mehrere Availability Zones hinweg bereitgestellt werden](#)
- [\[NetworkFirewall.2\] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein](#)

- [\[NetworkFirewall.3\] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet haben](#)
- [\[NetworkFirewall.4\] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ sein.](#)
- [\[NetworkFirewall.5\] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ sein.](#)
- [\[NetworkFirewall.6\] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein](#)
- [\[NetworkFirewall.7\] Netzwerk-Firewall-Firewalls sollten markiert werden](#)
- [\[NetworkFirewall.8\] Firewall-Richtlinien für Netzwerk-Firewalls sollten markiert werden](#)
- [\[NetworkFirewall.9\] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein](#)
- [\[NetworkFirewall.10\] Bei Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein](#)
- [Bei \[Opensearch.1\] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein](#)
- [\[Opensearch.2\] OpenSearch -Domains sollten nicht öffentlich zugänglich sein](#)
- [\[Opensearch.3\] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden](#)
- [Die Protokollierung von \[Opensearch.4\] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein](#)
- [Für \[Opensearch.5\] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein](#)
- [\[Opensearch.6\] OpenSearch Domains sollten mindestens drei Datenknoten haben](#)
- [Für \[Opensearch.7\] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein](#)
- [\[Opensearch.8\] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden](#)
- [\[Opensearch.9\] OpenSearch -Domains sollten mit Tags versehen werden](#)
- [Auf \[Opensearch.10\] OpenSearch -Domains sollte das neueste Softwareupdate installiert sein](#)
- [\[Opensearch.11\] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben](#)
- [\[PCA.1\] AWS Private CA Root-Zertifizierungsstelle sollte deaktiviert sein](#)
- [\[PCA.2\] AWS Private CA-Zertifizierungsstellen sollten gekennzeichnet werden](#)
- [\[RDS.14\] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein](#)
- [\[RDS.16\] Aurora-DB-Cluster sollten so konfiguriert sein, dass sie Tags in DB-Snapshots kopieren](#)
- [\[RDS.17\] RDS-DB-Instances sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren](#)

- [\[RDS.18\] RDS-Instances sollten in einer VPC bereitgestellt werden](#)
- [\[RDS.19\] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Cluster-Ereignisse konfiguriert werden](#)
- [\[RDS.20\] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Ereignisse der Datenbankinstanz konfiguriert werden](#)
- [\[RDS.21\] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbankparametergruppenereignisse konfiguriert werden](#)
- [\[RDS.22\] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbanksicherheitsgruppenereignisse konfiguriert werden](#)
- [\[RDS.23\] RDS-Instances sollten keinen Standard-Port für die Datenbank-Engine verwenden](#)
- [\[RDS.24\] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden](#)
- [\[RDS.25\] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden](#)
- [\[RDS.26\] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden](#)
- [\[RDS.27\] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[RDS.28\] RDS-DB-Cluster sollten markiert werden](#)
- [\[RDS.29\] RDS-DB-Cluster-Snapshots sollten markiert werden](#)
- [\[RDS.30\] RDS-DB-Instances sollten markiert werden](#)
- [\[RDS.31\] RDS-DB-Sicherheitsgruppen sollten markiert werden](#)
- [\[RDS.32\] RDS-DB-Snapshots sollten markiert werden](#)
- [\[RDS.33\] RDS-DB-Subnetzgruppen sollten markiert werden](#)
- [\[RDS.34\] Aurora MySQL-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)
- [\[RDS.35\] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein](#)
- [\[RDS.36\] RDS für PostgreSQL-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[RDS.37\] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[RDS.38\] RDS für PostgreSQL-DB-Instances sollten bei der Übertragung verschlüsselt werden](#)
- [\[RDS.39\] RDS für MySQL-DB-Instances sollten bei der Übertragung verschlüsselt werden](#)
- [\[RDS.40\] RDS für SQL Server-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[RDS.41\] RDS für SQL Server-DB-Instances sollten bei der Übertragung verschlüsselt werden](#)
- [\[RDS.42\] RDS für MariaDB-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch](#)

- [\[RDS.44\] RDS für MariaDB-DB-Instances sollte bei der Übertragung verschlüsselt werden](#)
- [\[RDS.45\] Bei Aurora MySQL-DB-Clustern sollte die Audit-Protokollierung aktiviert sein](#)
- [\[Redshift.1\] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten](#)
- [\[Redshift.2\] Verbindungen zu Amazon Redshift Redshift-Clustern sollten bei der Übertragung verschlüsselt werden](#)
- [\[Redshift.3\] Bei Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein](#)
- [\[Redshift.4\] Bei Amazon Redshift Redshift-Clustern sollte die Auditprotokollierung aktiviert sein](#)
- [\[Redshift.6\] Bei Amazon Redshift sollten automatische Upgrades auf Hauptversionen aktiviert sein](#)
- [\[Redshift.7\] Redshift-Cluster sollten erweitertes VPC-Routing verwenden](#)
- [\[Redshift.8\] Amazon Redshift Redshift-Cluster sollten nicht den standardmäßigen Admin-Benutzernamen verwenden](#)
- [\[Redshift.9\] Redshift-Cluster sollten nicht den Standard-Datenbanknamen verwenden](#)
- [\[Redshift.10\] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[Redshift.11\] Redshift-Cluster sollten markiert werden](#)
- [\[Redshift.12\] Abonnements für Redshift-Ereignisbenachrichtigungen sollten markiert werden](#)
- [\[Redshift.13\] Redshift-Cluster-Snapshots sollten markiert werden](#)
- [\[Redshift.14\] Redshift-Cluster-Subnetzgruppen sollten markiert werden](#)
- [\[Redshift.15\] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen](#)
- [\[Redshift.16\] Redshift-Cluster-Subnetzgruppen sollten Subnetze aus mehreren Availability Zones haben](#)
- [\[Redshift.17\] Redshift-Cluster-Parametergruppen sollten markiert werden](#)
- [\[Redshift.18\] Für Redshift-Cluster sollten Multi-AZ-Bereitstellungen aktiviert sein](#)
- [\[RedshiftServerless.1\] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden](#)
- [\[RedshiftServerless.2\] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein](#)
- [\[RedshiftServerless.3\] Serverlose Redshift-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten](#)
- [\[RedshiftServerless.4\] Serverlose Redshift-Namespace sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys](#)
- [\[RedshiftServerless.5\] Redshift Serverless-Namespace sollten nicht den Standard-Admin-Benutzernamen verwenden](#)

- [\[RedshiftServerless.6\] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch](#)
- [\[RedshiftServerless.7\] Redshift Serverless-Namespaces sollten nicht den Standard-Datenbanknamen verwenden](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.7\] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden](#)
- [\[S3.10\] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben](#)
- [\[S3.11\] Bei S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein](#)
- [\[S3.12\] ACLs sollte nicht zur Verwaltung des Benutzerzugriffs auf S3-Allzweck-Buckets verwendet werden](#)
- [\[S3.13\] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben](#)
- [\[S3.19\] Bei S3-Zugriffspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.20\] Bei S3-Allzweck-Buckets sollte MFA Delete aktiviert sein](#)
- [\[S3.22\] S3-Allzweck-Buckets sollten Schreibereignisse auf Objektebene protokollieren](#)
- [\[S3.23\] S3-Allzweck-Buckets sollten Leseereignisse auf Objektebene protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)
- [\[SageMaker.1\] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben](#)
- [\[SageMaker.2\] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden](#)
- [\[SageMaker.3\] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben](#)
- [\[SageMaker.4\] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein](#)
- [\[SageMaker.5\] SageMaker Modelle sollten eingehenden Datenverkehr blockieren](#)
- [\[SageMaker.6\] SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden](#)
- [\[SageMaker.7\] SageMaker Bilder sollten mit Tags versehen werden](#)
- [\[SageMaker.8\] SageMaker Notebook-Instances sollten auf unterstützten Plattformen laufen](#)

- [\[SES.1\] SES-Kontaktlisten sollten mit Tags versehen werden](#)
- [\[SES.2\] SES-Konfigurationssätze sollten mit Tags versehen werden](#)
- [\[SecretsManager.5\] Secrets Manager Manager-Geheimnisse sollten markiert werden](#)
- [\[ServiceCatalog.1\] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden](#)
- [\[SNS.3\] SNS-Themen sollten markiert werden](#)
- [\[SNS.4\] Zugriffsrichtlinien für SNS-Themen sollten keinen öffentlichen Zugriff zulassen](#)
- [\[SQS.1\] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt werden](#)
- [\[SQS.2\] SQS-Warteschlangen sollten markiert werden](#)
- [\[SQS.3\] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen](#)
- [\[SSM.3\] Von Systems Manager verwaltete EC2 Amazon-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben](#)
- [\[SSM.4\] SSM-Dokumente sollten nicht öffentlich sein](#)
- [\[SSM.5\] SSM-Dokumente sollten mit Tags versehen werden](#)
- [\[SSM.6\] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[SSM.7\] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein](#)
- [\[StepFunctions.1\] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben](#)
- [\[StepFunctions.2\] Die Aktivitäten von Step Functions sollten mit Tags versehen werden](#)
- [\[Transfer.1\] AWS Transfer Family -Workflows sollten mit Tags versehen werden](#)
- [\[Transfer.2\] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden](#)
- [\[Transfer.3\] Bei Connectoren der Transfer-Familie sollte die Protokollierung aktiviert sein](#)
- [\[Transfer.4\] Transfer Family Familienverträge sollten gekennzeichnet werden](#)
- [\[Transfer.5\] Transfer Family Familienzertifikate sollten gekennzeichnet sein](#)
- [\[Transfer.6\] Steckverbinder der Transfer-Familie sollten gekennzeichnet sein](#)
- [\[Transfer.7\] Familienprofile sollten mit Tags versehen werden](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.2\] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.3\] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben](#)

- [\[WAF.4\] AWS WAF Classic Regional Web ACLs sollte mindestens eine Regel oder Regelgruppe enthalten](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WAF.10\] AWS WAF web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WAF.11\] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein](#)
- [Für \[WAF.12\] AWS WAF Regeln sollten Metriken aktiviert sein CloudWatch](#)
- [\[WorkSpaces.1\] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden](#)
- [\[WorkSpaces.2\] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden](#)

Asien-Pazifik (Tokio)

Die folgenden Steuerelemente werden in der Region Asien-Pazifik (Tokio) nicht unterstützt.

- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)

- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[ECR.4\] Öffentliche ECR-Repositoryn sollten markiert werden](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[IoT Twin Maker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)

Kanada (Zentral)

Die folgenden Steuerelemente werden in der Region Kanada (Mitte) nicht unterstützt.

- [\[AppRunner.1\] App Runner-Dienste sollten markiert sein](#)
- [\[AppRunner.2\] App Runner VPC-Konnektoren sollten markiert sein](#)
- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)

- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[CodeArtifact.1\] CodeArtifact Repositorien sollten mit Tags versehen werden](#)
- [\[CodeGuruProfiler.1\] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden](#)
- [\[CodeGuruReviewer.1\] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden](#)
- [\[DynamoDB.3\] DynamoDB Accelerator \(DAX\) -Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DynamoDB.7\] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[EC2.24\] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[ECR.4\] Öffentliche ECR-Repositorien sollten markiert werden](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)

- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)
- [\[IoT Twin Maker.1\] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden](#)
- [\[IoT Twin Maker.2\] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden](#)
- [\[IoT Twin Maker.3\] AWS TwinMaker IoT-Szenen sollten markiert werden](#)
- [\[IoT Twin Maker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[IoT Wireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[IoT Wireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)
- [\[IoT Wireless .3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)
- [\[Kinesis.3\] Kinesis-Streams sollten über eine angemessene Aufbewahrungsfrist für Daten verfügen](#)
- [\[RDS.31\] RDS-DB-Sicherheitsgruppen sollten markiert werden](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)

Kanada West (Calgary)

Die folgenden Steuerelemente werden in der Region Kanada West (Calgary) nicht unterstützt.

- [\[ACM.1\] Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden](#)
- [\[ACM.2\] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden](#)
- [\[Account.1\] Sicherheitskontaktinformationen sollten bereitgestellt werden für AWS-Konto](#)
- [\[Account.2\] AWS-Konten sollte Teil einer Organisation sein AWS Organizations](#)
- [\[APIGateway.8\] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben](#)
- [\[APIGateway.9\] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein](#)
- [\[Amplify.1\] Amplify-Apps sollten markiert werden](#)
- [\[Amplify.2\] Amplify-Zweige sollten markiert werden](#)
- [\[AppConfig.1\] AWS AppConfig Anwendungen sollten markiert werden](#)
- [\[AppConfig.2\] AWS AppConfig Konfigurationsprofile sollten mit Tags versehen werden](#)
- [\[AppConfig.3\] AWS AppConfig Umgebungen sollten markiert werden](#)
- [\[AppConfig.4\] AWS AppConfig Erweiterungszuordnungen sollten markiert werden](#)
- [\[AppFlow.1\] AppFlow Amazon-Datenflüsse sollten mit Tags versehen werden](#)
- [\[AppRunner.1\] App Runner-Dienste sollten markiert sein](#)
- [\[AppRunner.2\] App Runner VPC-Konnektoren sollten markiert sein](#)
- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.2\] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben](#)
- [\[AppSync.4\] AWS AppSync GraphQL APIs sollte markiert sein](#)
- [\[AppSync.5\] AWS AppSync GraphQL APIs sollte nicht mit API-Schlüsseln authentifiziert werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [\[Athena.4\] Bei Athena-Arbeitsgruppen sollte die Protokollierung aktiviert sein](#)
- [\[AutoScaling.2\] Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken](#)
- [\[AutoScaling.3\] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2 Instances so konfigurieren, dass sie Instance Metadata Service Version 2 \(IMDSv2\) benötigen](#)
- [\[AutoScaling.6\] Auto Scaling Scaling-Gruppen sollten mehrere Instance-Typen in mehreren Availability Zones verwenden](#)
- [\[AutoScaling.9\] Amazon EC2 Auto Scaling Scaling-Gruppen sollten EC2 Amazon-Startvorlagen verwenden](#)

- [\[Backup.1\] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein](#)
- [\[Backup.4\] AWS Backup Berichtspläne sollten markiert werden](#)
- [\[Batch.1\] Warteschlangen für Batch-Jobs sollten markiert werden](#)
- [\[Batch.3\] Batch-Computing-Umgebungen sollten markiert werden](#)
- [\[Batch.4\] Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[CloudTrail.6\] Sicherstellen, dass der S3-Bucket, in dem CloudTrail Protokolle gespeichert werden, nicht öffentlich zugänglich ist](#)
- [\[CloudTrail.7\] Sicherstellen, dass die S3-Bucket-Zugriffsprotokollierung für den CloudTrail S3-Bucket aktiviert ist](#)
- [\[CloudTrail.10\] Event-Datenspeicher in CloudTrail Lake sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys](#)
- [\[CloudWatch.17\] CloudWatch Alarmaktionen sollten aktiviert sein](#)

- [\[CodeArtifact.1\] CodeArtifact Repositorien sollten mit Tags versehen werden](#)
- [\[CodeBuild.1\] Das CodeBuild Bitbucket-Quell-Repository URLs sollte keine vertraulichen Anmeldeinformationen enthalten](#)
- [\[CodeBuild.2\] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten](#)
- [\[CodeBuild.3\] CodeBuild S3-Protokolle sollten verschlüsselt sein](#)
- [\[CodeBuild.4\] CodeBuild Projektumgebungen sollten eine AWS Config Protokollierungsdauer haben](#)
- [\[CodeBuild.7\] Exporte von CodeBuild Berichtsgruppen sollten im Ruhezustand verschlüsselt werden](#)
- [\[CodeGuruProfiler.1\] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden](#)
- [\[CodeGuruReviewer.1\] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden](#)
- [\[Cognito.1\] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein](#)
- [\[Cognito.2\] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen](#)
- [\[Connect.1\] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden](#)
- [\[Connect.2\] Für Amazon Connect Connect-Instances sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[DataFirehose.1\] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden](#)
- [\[DataSync.1\] Für DataSync Aufgaben sollte die Protokollierung aktiviert sein](#)
- [\[Detective.1\] Verhaltensdiagramme von Detektiven sollten markiert werden](#)
- [\[DMS.2\] DMS-Zertifikate sollten gekennzeichnet sein](#)
- [\[DMS.3\] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden](#)
- [\[DMS.4\] DMS-Replikationsinstanzen sollten markiert werden](#)
- [\[DMS.5\] Subnetzgruppen für die DMS-Replikation sollten markiert werden](#)
- [\[DMS.6\] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein](#)
- [\[DMS.7\] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.8\] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.9\] DMS-Endpunkte sollten SSL verwenden](#)

- [\[DMS.10\] Bei DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein](#)
- [\[DMS.11\] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein](#)
- [\[DMS.12\] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein](#)
- [\[DocumentDB.1\] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DocumentDB.2\] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen](#)
- [\[DocumentDB.3\] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein](#)
- [\[DocumentDB.4\] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch](#)
- [\[DocumentDB.5\] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[DocumentDB.6\] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[DynamoDB.3\] DynamoDB Accelerator \(DAX\) -Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DynamoDB.4\] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein](#)
- [\[DynamoDB.6\] Bei DynamoDB-Tabellen sollte der Löschschutz aktiviert sein](#)
- [\[DynamoDB.7\] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[EC2.4\] Gestoppte EC2 Instances sollten nach einem bestimmten Zeitraum entfernt werden](#)
- [\[EC2.21\] Das Netzwerk ACLs sollte keinen Zugang von 0.0.0.0/0 zu Port 22 oder Port 3389 zulassen](#)
- [\[EC2.22\] Ungenutzte EC2 Amazon-Sicherheitsgruppen sollten entfernt werden](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways sollte VPC-Anhangsanfragen nicht automatisch akzeptieren](#)
- [\[EC2.24\] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden](#)
- [\[EC2.25\] EC2 Amazon-Startvorlagen sollten Netzwerkschnittstellen nicht öffentlich IPs zuweisen](#)
- [\[EC2.28\] EBS-Volumes sollten durch einen Backup-Plan abgedeckt sein](#)
- [\[EC2.33\] EC2 Transit-Gateway-Anhänge sollten mit Tags versehen werden](#)
- [\[EC2.34\] Die Routentabellen für EC2 Transit-Gateways sollten mit Tags versehen werden](#)
- [\[EC2.40\] EC2 NAT-Gateways sollten markiert werden](#)
- [\[EC2.48\] Amazon VPC-Flow-Logs sollten mit Tags versehen werden](#)

- [\[EC2.51\] EC2 Client-VPN-Endpunkte sollten die Client-Verbindungsprotokollierung aktiviert haben](#)
- [\[EC2.53\] EC2 Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 zu Remote-Serververwaltungsports zulassen](#)
- [\[EC2.54\] EC2 Sicherheitsgruppen sollten keinen Zugriff von: :/0 zu Remote-Serveradministrationsports zulassen](#)
- [\[EC2.55\] VPCs sollte mit einem Schnittstellenendpunkt für die ECR-API konfiguriert werden](#)
- [\[EC2.56\] VPCs sollte mit einem Schnittstellenendpunkt für Docker Registry konfiguriert werden](#)
- [\[EC2.57\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager konfiguriert werden](#)
- [\[EC2.58\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert sein](#)
- [\[EC2.60\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden](#)
- [\[EC2.170\] EC2 Startvorlagen sollten Instance Metadata Service Version 2 \(\) verwenden IMDSv2](#)
- [\[EC2.171\] Bei EC2 VPN-Verbindungen sollte die Protokollierung aktiviert sein](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[EC2.175\] EC2 Startvorlagen sollten mit Tags versehen sein](#)
- [\[EC2.177\] EC2 Traffic Mirror-Sitzungen sollten mit Tags versehen werden](#)
- [\[EC2.179\] EC2 Traffic-Spiegel-Ziele sollten markiert werden](#)
- [\[EC2.180\] Bei EC2 Netzwerkschnittstellen sollte die source/destination Überprüfung aktiviert sein](#)
- [\[ECR.1\] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein](#)
- [\[ECR.2\] Bei privaten ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein](#)
- [\[ECR.3\] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein](#)
- [\[ECR.4\] Öffentliche ECR-Repositorys sollten markiert werden](#)
- [\[ECR.5\] ECR-Repositorys sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys](#)
- [\[ECS.3\] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen](#)
- [\[ECS.4\] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden](#)
- [\[ECS.5\] ECS-Container sollten auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sein](#)
- [\[ECS.8\] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden](#)

- [\[ECS.9\] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen](#)
- [\[ECS.10\] Die ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen](#)
- [\[ECS.12\] ECS-Cluster sollten Container Insights verwenden](#)
- [\[ECS.16\] ECS-Aufgabensätze sollten öffentliche IP-Adressen nicht automatisch zuweisen](#)
- [\[ECS.17\] ECS-Aufgabendefinitionen sollten nicht den Host-Netzwerkmodus verwenden](#)
- [\[EFS.1\] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS](#)
- [\[EFS.2\] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein](#)
- [\[EFS.3\] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen](#)
- [\[EFS.4\] EFS-Zugangspunkte sollten eine Benutzeridentität erzwingen](#)
- [\[EFS.6\] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden](#)
- [\[EFS.7\] Bei EFS-Dateisystemen sollten automatische Backups aktiviert sein](#)
- [\[EFS.8\] EFS-Dateisysteme sollten im Ruhezustand verschlüsselt werden](#)
- [\[EKS.2\] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden](#)
- [\[EKS.3\] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden](#)
- [\[EKS.6\] EKS-Cluster sollten markiert werden](#)
- [\[EKS.7\] Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden](#)
- [\[EKS.8\] Bei EKS-Clustern sollte die Auditprotokollierung aktiviert sein](#)
- [\[ELB.2\] Classic Load Balancer mit SSL/HTTPS Listnern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager](#)
- [\[ELB.10\] Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken](#)
- [\[ELB.12\] Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden](#)
- [\[ELB.13\] Anwendungs-, Netzwerk- und Gateway-Load Balancer sollten sich über mehrere Availability Zones erstrecken](#)
- [\[ELB.14\] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden](#)
- [\[ELB.17\] Anwendungs- und Netzwerk-Load-Balancer mit Listnern sollten die empfohlenen Sicherheitsrichtlinien verwenden](#)
- [\[ELB.18\] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln](#)
- [Bei \[ElastiCache.1\] ElastiCache \(Redis OSS\) -Clustern sollten automatische Backups aktiviert sein](#)

- [\[ElastiCache.2\] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein](#)
- [\[ElastiCache.3\] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein](#)
- [\[ElastiCache.4\] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden](#)
- [\[ElastiCache.5\] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden](#)
- [\[ElastiCache.6\] Für Replikationsgruppen ElastiCache \(Redis OSS\) früherer Versionen sollte Redis OSS AUTH aktiviert sein](#)
- [\[ElastiCache.7\] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden](#)
- [\[ElasticBeanstalk.1\] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben](#)
- [\[ElasticBeanstalk.2\] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk sollte Logs streamen nach CloudWatch](#)
- [\[EMR.1\] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben](#)
- [\[EMR.2\] Die Amazon EMR-Einstellung zum Blockieren des öffentlichen Zugriffs sollte aktiviert sein](#)
- [\[EMR.3\] Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden](#)
- [\[ES.3\] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden](#)
- [\[ES.4\] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein](#)
- [\[EventBridge.3\] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden](#)
- [\[EventBridge.4\] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[FSx.1\] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden](#)
- [\[FSx.2\] FSx für Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden](#)
- [\[FSx.3\] FSx für OpenZFS-Dateisysteme sollte für die Multi-AZ-Bereitstellung konfiguriert werden](#)
- [\[FSx.4\] FSx für NetApp ONTAP-Dateisysteme sollte für die Multi-AZ-Bereitstellung konfiguriert sein](#)
- [\[FSx.5\] FSx für Windows-Dateiserver sollten für die Multi-AZ-Bereitstellung konfiguriert sein](#)

- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[Glue.3\] Transformationen für AWS Glue maschinelles Lernen sollten im Ruhezustand verschlüsselt werden](#)
- [\[Glue.4\] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue](#)
- [\[GuardDuty.2\] GuardDuty Filter sollten mit Tags versehen sein](#)
- [\[GuardDuty.3\] GuardDuty IPSets sollte markiert werden](#)
- [\[GuardDuty.5\] GuardDuty EKS Audit Log Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.6\] GuardDuty Lambda Protection sollte aktiviert sein](#)
- [\[GuardDuty.7\] GuardDuty EKS Runtime Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.8\] Der GuardDuty Malware-Schutz für EC2 sollte aktiviert sein](#)
- [\[GuardDuty.9\] Der GuardDuty RDS-Schutz sollte aktiviert sein](#)
- [\[GuardDuty.10\] Der GuardDuty S3-Schutz sollte aktiviert sein](#)
- [\[GuardDuty.11\] GuardDuty Runtime Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.12\] GuardDuty ECS Runtime Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.13\] GuardDuty EC2 Runtime Monitoring sollte aktiviert sein](#)
- [\[IAM.1\] IAM-Richtlinien sollten keine vollen „*“-Administratorrechte zulassen](#)
- [\[IAM.2\] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein](#)
- [\[IAM.3\] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden](#)
- [\[IAM.4\] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren](#)
- [\[IAM.5\] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen](#)
- [\[IAM.6\] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.](#)
- [\[IAM.7\] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein](#)
- [\[IAM.8\] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden](#)
- [\[IAM.9\] MFA sollte für den Root-Benutzer aktiviert sein](#)
- [\[IAM.10\] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein](#)
- [\[IAM.11\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert](#)
- [\[IAM.12\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert](#)

- [\[IAM.13\] Stellen Sie sicher, dass für die IAM-Passwortrichtlinie mindestens ein Symbol erforderlich ist](#)
- [\[IAM.14\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert](#)
- [\[IAM.15\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert](#)
- [\[IAM.16\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert](#)
- [\[IAM.17\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft](#)
- [\[IAM.18\] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS -Support](#)
- [\[IAM.19\] MFA sollte für alle IAM-Benutzer aktiviert sein](#)
- [\[IAM.21\] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen](#)
- [\[IAM.22\] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden](#)
- [\[IAM.24\] IAM-Rollen sollten mit Tags versehen werden](#)
- [\[IAM.25\] IAM-Benutzer sollten markiert werden](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[IAM.27\] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWS Cloud Shell FullAccess](#)
- [\[IAM.28\] Der externe Zugriffsanalysator für IAM Access Analyzer sollte aktiviert sein](#)
- [\[Inspector.1\] Das EC2 Scannen mit Amazon Inspector sollte aktiviert sein](#)
- [\[Inspector.2\] Das Amazon Inspector ECR-Scannen sollte aktiviert sein](#)
- [\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)
- [\[Inspector.4\] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein](#)
- [\[IoT.1\] AWS IoT Device Defender Sicherheitsprofile sollten markiert werden](#)
- [\[IoT.2\] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden](#)
- [\[IoT.3\] AWS IoT Core -Dimensionen sollten markiert werden](#)
- [\[IoT.4\] AWS IoT Core Autorisierer sollten markiert werden](#)
- [\[IoT.5\] AWS IoT Core Rollenalias sollten markiert werden](#)
- [\[IoT.6\] AWS IoT Core Richtlinien sollten markiert werden](#)

- [\[Io TEvents .1\] AWS IoT-Events-Eingaben sollten markiert werden](#)
- [\[Io TEvents .2\] AWS IoT-Ereignisdetektormodelle sollten markiert werden](#)
- [\[Io TEvents .3\] Alarmmodelle für AWS IoT Events sollten markiert werden](#)
- [\[Io TSite Wise.1\] AWS SiteWise IoT-Asset-Modelle sollten markiert werden](#)
- [\[Io TSite Wise.2\] AWS SiteWise IoT-Dashboards sollten markiert werden](#)
- [\[Io TSite Wise.3\] AWS SiteWise IoT-Gateways sollten markiert werden](#)
- [\[Io TSite Wise.4\] AWS SiteWise IoT-Portale sollten markiert werden](#)
- [\[Io TSite Wise.5\] AWS SiteWise IoT-Projekte sollten markiert werden](#)
- [\[Io TTwin Maker.1\] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden](#)
- [\[Io TTwin Maker.2\] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden](#)
- [\[Io TTwin Maker.3\] AWS TwinMaker IoT-Szenen sollten markiert werden](#)
- [\[Io TTwin Maker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[Io TWireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[Io TWireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)
- [\[Io TWireless .3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)
- [\[Keyspaces.1\] Amazon Keyspaces Keyspaces sollten mit Tags versehen sein](#)
- [\[Kinesis.1\] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden](#)
- [\[Kinesis.2\] Kinesis-Streams sollten markiert werden](#)
- [\[Kinesis.3\] Kinesis-Streams sollten über eine angemessene Aufbewahrungsfrist für Daten verfügen](#)
- [\[KMS.1\] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)
- [\[KMS.2\] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)
- [\[KMS.5\] KMS-Schlüssel sollten nicht öffentlich zugänglich sein](#)
- [\[Lambda.5\] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren](#)
- [\[Lambda.7\] Bei Lambda-Funktionen sollte aktives Tracing aktiviert sein AWS X-Ray](#)
- [\[Macie.1\] Amazon Macie sollte aktiviert sein](#)

- [\[Macie.2\] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein](#)
- [\[MQ.2\] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch](#)
- [\[MQ.3\] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein](#)
- [\[MQ.4\] Amazon MQ-Broker sollten markiert werden](#)
- [\[MQ.5\] ActiveMQ-Broker sollten den Aktiv-/Standby-Bereitstellungsmodus verwenden](#)
- [\[MQ.6\] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden](#)
- [\[MSK.1\] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden](#)
- [\[MSK.2\] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein](#)
- [\[MSK.3\] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden](#)
- [\[MSK.4\] Bei MSK-Clustern sollte der öffentliche Zugriff deaktiviert sein](#)
- [\[MSK.5\] Bei MSK-Konnektoren sollte die Protokollierung aktiviert sein](#)
- [\[MSK.6\] MSK-Cluster sollten den nicht authentifizierten Zugriff deaktivieren](#)
- [\[Neptune.1\] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.2\] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)
- [\[Neptune.3\] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein](#)
- [\[Neptune.4\] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[Neptune.5\] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein](#)
- [\[Neptune.6\] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.7\] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein](#)
- [\[Neptune.8\] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren](#)
- [\[Neptune.9\] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden](#)
- [\[NetworkFirewall.1\] Network firewalls sollten über mehrere Availability Zones hinweg bereitgestellt werden](#)
- [\[NetworkFirewall.2\] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein](#)
- [\[NetworkFirewall.3\] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet haben](#)
- [\[NetworkFirewall.4\] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ sein.](#)
- [\[NetworkFirewall.5\] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ sein.](#)
- [\[NetworkFirewall.6\] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein](#)

- [\[NetworkFirewall.9\] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein](#)
- [\[NetworkFirewall.10\] Bei Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein](#)
- [Bei \[Opensearch.1\] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein](#)
- [\[Opensearch.2\] OpenSearch -Domains sollten nicht öffentlich zugänglich sein](#)
- [\[Opensearch.3\] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden](#)
- [Die Protokollierung von \[Opensearch.4\] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein](#)
- [Für \[Opensearch.5\] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein](#)
- [\[Opensearch.6\] OpenSearch Domains sollten mindestens drei Datenknoten haben](#)
- [Für \[Opensearch.7\] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein](#)
- [\[Opensearch.8\] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden](#)
- [\[Opensearch.9\] OpenSearch -Domains sollten mit Tags versehen werden](#)
- [Auf \[Opensearch.10\] OpenSearch -Domains sollte das neueste Softwareupdate installiert sein](#)
- [\[Opensearch.11\] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben](#)
- [\[PCA.1\] AWS Private CA Root-Zertifizierungsstelle sollte deaktiviert sein](#)
- [\[RDS.14\] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein](#)
- [\[RDS.18\] RDS-Instances sollten in einer VPC bereitgestellt werden](#)
- [\[RDS.24\] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden](#)
- [\[RDS.25\] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden](#)
- [\[RDS.26\] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden](#)
- [\[RDS.27\] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[RDS.31\] RDS-DB-Sicherheitsgruppen sollten markiert werden](#)
- [\[RDS.34\] Aurora MySQL-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)
- [\[RDS.35\] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein](#)
- [\[RDS.36\] RDS für PostgreSQL-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[RDS.37\] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch](#)

- [\[RDS.38\] RDS für PostgreSQL-DB-Instances sollten bei der Übertragung verschlüsselt werden](#)
- [\[RDS.39\] RDS für MySQL-DB-Instances sollten bei der Übertragung verschlüsselt werden](#)
- [\[RDS.40\] RDS für SQL Server-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[RDS.41\] RDS für SQL Server-DB-Instances sollten bei der Übertragung verschlüsselt werden](#)
- [\[RDS.42\] RDS für MariaDB-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[RDS.44\] RDS für MariaDB-DB-Instances sollte bei der Übertragung verschlüsselt werden](#)
- [\[RDS.45\] Bei Aurora MySQL-DB-Clustern sollte die Audit-Protokollierung aktiviert sein](#)
- [\[Redshift.3\] Bei Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein](#)
- [\[Redshift.6\] Bei Amazon Redshift sollten automatische Upgrades auf Hauptversionen aktiviert sein](#)
- [\[Redshift.7\] Redshift-Cluster sollten erweitertes VPC-Routing verwenden](#)
- [\[Redshift.8\] Amazon Redshift Redshift-Cluster sollten nicht den standardmäßigen Admin-Benutzernamen verwenden](#)
- [\[Redshift.9\] Redshift-Cluster sollten nicht den Standard-Datenbanknamen verwenden](#)
- [\[Redshift.10\] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[Redshift.15\] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen](#)
- [\[Redshift.16\] Redshift-Cluster-Subnetzgruppen sollten Subnetze aus mehreren Availability Zones haben](#)
- [\[Redshift.18\] Für Redshift-Cluster sollten Multi-AZ-Bereitstellungen aktiviert sein](#)
- [\[RedshiftServerless.1\] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden](#)
- [\[RedshiftServerless.2\] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein](#)
- [\[RedshiftServerless.3\] Serverlose Redshift-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten](#)
- [\[RedshiftServerless.4\] Serverlose Redshift-Namespace sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys](#)
- [\[RedshiftServerless.5\] Redshift Serverless-Namespace sollten nicht den Standard-Admin-Benutzernamen verwenden](#)
- [\[RedshiftServerless.6\] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch](#)
- [\[RedshiftServerless.7\] Redshift Serverless-Namespace sollten nicht den Standard-Datenbanknamen verwenden](#)

- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.7\] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden](#)
- [\[S3.10\] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben](#)
- [\[S3.11\] Bei S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein](#)
- [\[S3.12\] ACLs sollte nicht zur Verwaltung des Benutzerzugriffs auf S3-Allzweck-Buckets verwendet werden](#)
- [\[S3.13\] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben](#)
- [\[S3.19\] Bei S3-Zugriffspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.20\] Bei S3-Allzweck-Buckets sollte MFA Delete aktiviert sein](#)
- [\[S3.22\] S3-Allzweck-Buckets sollten Schreibereignisse auf Objektebene protokollieren](#)
- [\[S3.23\] S3-Allzweck-Buckets sollten Leseereignisse auf Objektebene protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)
- [\[SageMaker.1\] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben](#)
- [\[SageMaker.2\] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden](#)
- [\[SageMaker.3\] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben](#)
- [\[SageMaker.4\] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein](#)
- [\[SageMaker.5\] SageMaker Modelle sollten eingehenden Datenverkehr blockieren](#)
- [\[SageMaker.6\] SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden](#)
- [\[SageMaker.7\] SageMaker Bilder sollten mit Tags versehen werden](#)
- [\[SageMaker.8\] SageMaker Notebook-Instances sollten auf unterstützten Plattformen laufen](#)
- [\[SES.1\] SES-Kontaktlisten sollten mit Tags versehen werden](#)
- [\[SES.2\] SES-Konfigurationssätze sollten mit Tags versehen werden](#)
- [\[ServiceCatalog.1\] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden](#)

- [\[SNS.4\] Zugriffsrichtlinien für SNS-Themen sollten keinen öffentlichen Zugriff zulassen](#)
- [\[SQS.1\] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt werden](#)
- [\[SQS.2\] SQS-Warteschlangen sollten markiert werden](#)
- [\[SQS.3\] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen](#)
- [\[SSM.2\] Von Systems Manager verwaltete EC2 Amazon-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben](#)
- [\[SSM.3\] Von Systems Manager verwaltete EC2 Amazon-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben](#)
- [\[SSM.4\] SSM-Dokumente sollten nicht öffentlich sein](#)
- [\[SSM.6\] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[SSM.7\] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein](#)
- [\[StepFunctions.1\] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben](#)
- [\[Transfer.2\] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden](#)
- [\[Transfer.3\] Bei Connectoren der Transfer-Familie sollte die Protokollierung aktiviert sein](#)
- [\[Transfer.4\] Transfer Family Familienverträge sollten gekennzeichnet werden](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.2\] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.3\] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.4\] AWS WAF Classic Regional Web ACLs sollte mindestens eine Regel oder Regelgruppe enthalten](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WAF.10\] AWS WAF web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WAF.11\] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein](#)
- [Für \[WAF.12\] AWS WAF Regeln sollten Metriken aktiviert sein CloudWatch](#)
- [\[WorkSpaces.1\] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden](#)

- [\[WorkSpaces.2\] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden](#)

China (Peking)

Die folgenden Steuerelemente werden in der Region China (Peking) nicht unterstützt.

- [\[ACM.1\] Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden](#)
- [\[ACM.2\] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden](#)
- [\[Account.2\] AWS-Konten sollte Teil einer Organisation sein AWS Organizations](#)
- [\[APIGateway.2\] API Gateway REST API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden](#)
- [\[Amplify.1\] Amplify-Apps sollten markiert werden](#)
- [\[Amplify.2\] Amplify-Zweige sollten markiert werden](#)
- [\[AppConfig.1\] AWS AppConfig Anwendungen sollten markiert werden](#)
- [\[AppConfig.2\] AWS AppConfig Konfigurationsprofile sollten mit Tags versehen werden](#)
- [\[AppConfig.3\] AWS AppConfig Umgebungen sollten markiert werden](#)
- [\[AppConfig.4\] AWS AppConfig Erweiterungszuordnungen sollten markiert werden](#)
- [\[AppFlow.1\] AppFlow Amazon-Datenflüsse sollten mit Tags versehen werden](#)
- [\[AppRunner.1\] App Runner-Dienste sollten markiert sein](#)
- [\[AppRunner.2\] App Runner VPC-Konnektoren sollten markiert sein](#)
- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [\[AutoScaling.10\] EC2 Auto Scaling Scaling-Gruppen sollten markiert werden](#)
- [\[Backup.1\] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein](#)
- [\[Backup.4\] AWS Backup Berichtspläne sollten markiert werden](#)
- [\[Batch.1\] Warteschlangen für Batch-Jobs sollten markiert werden](#)
- [\[Batch.2\] Richtlinien für die Batch-Planung sollten gekennzeichnet sein](#)
- [\[Batch.3\] Batch-Computing-Umgebungen sollten markiert werden](#)
- [\[Batch.4\] Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden](#)

- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[CloudTrail.10\] Event-Datenspeicher in CloudTrail Lake sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys](#)
- [\[CodeArtifact.1\] CodeArtifact Repositorien sollten mit Tags versehen werden](#)
- [\[CodeGuruProfiler.1\] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden](#)
- [\[CodeGuruReviewer.1\] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden](#)
- [\[Cognito.1\] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein](#)
- [\[Cognito.2\] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen](#)
- [\[Connect.1\] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden](#)
- [\[Connect.2\] Für Amazon Connect Connect-Instances sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[DataFirehose.1\] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden](#)
- [\[DataSync.2\] DataSync Aufgaben sollten mit Tags versehen werden](#)
- [\[Detective.1\] Verhaltensdiagramme von Detektiven sollten markiert werden](#)
- [\[DMS.4\] DMS-Replikationsinstanzen sollten markiert werden](#)

- [\[DMS.5\] Subnetzgruppen für die DMS-Replikation sollten markiert werden](#)
- [\[DMS.10\] Bei DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein](#)
- [\[DMS.11\] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein](#)
- [\[DMS.12\] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein](#)
- [\[DocumentDB.1\] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DocumentDB.2\] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen](#)
- [\[DocumentDB.3\] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein](#)
- [\[DocumentDB.4\] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch](#)
- [\[DocumentDB.5\] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[DynamoDB.3\] DynamoDB Accelerator \(DAX\) -Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DynamoDB.4\] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein](#)
- [\[DynamoDB.7\] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[EC2.15\] EC2 Amazon-Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen](#)
- [\[EC2.16\] Ungenutzte Network Access Control Lists sollten entfernt werden](#)
- [\[EC2.20\] Beide VPN-Tunnel für eine AWS Site-to-Site VPN-Verbindung sollten aktiv sein](#)
- [\[EC2.22\] Ungenutzte EC2 Amazon-Sicherheitsgruppen sollten entfernt werden](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways sollte VPC-Anhangsanfragen nicht automatisch akzeptieren](#)
- [\[EC2.28\] EBS-Volumes sollten durch einen Backup-Plan abgedeckt sein](#)
- [\[EC2.33\] EC2 Transit-Gateway-Anhänge sollten mit Tags versehen werden](#)
- [\[EC2.34\] Die Routentabellen für EC2 Transit-Gateways sollten mit Tags versehen werden](#)
- [\[EC2.35\] EC2 Netzwerkschnittstellen sollten markiert werden](#)
- [\[EC2.36\] EC2 Kunden-Gateways sollten mit Tags versehen werden](#)
- [\[EC2.40\] EC2 NAT-Gateways sollten markiert werden](#)
- [\[EC2.41\] Das EC2 Netzwerk ACLs sollte markiert sein](#)
- [\[EC2.42\] EC2 Routing-Tabellen sollten mit Tags versehen werden](#)

- [\[EC2.43\] EC2 Sicherheitsgruppen sollten markiert werden](#)
- [\[EC2.44\] EC2 Subnetze sollten markiert werden](#)
- [\[EC2.46\] Amazon VPCs sollte markiert werden](#)
- [\[EC2.47\] Amazon VPC Endpoint Services sollten markiert werden](#)
- [\[EC2.48\] Amazon VPC-Flow-Logs sollten mit Tags versehen werden](#)
- [\[EC2.49\] Amazon VPC-Peering-Verbindungen sollten markiert werden](#)
- [\[EC2.51\] EC2 Client-VPN-Endpunkte sollten die Client-Verbindungsprotokollierung aktiviert haben](#)
- [\[EC2.53\] EC2 Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 zu Remote-Serververwaltungsports zulassen](#)
- [\[EC2.54\] EC2 Sicherheitsgruppen sollten keinen Zugriff von: :/0 zu Remote-Serveradministrationsports zulassen](#)
- [\[EC2.58\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert sein](#)
- [\[EC2.60\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden](#)
- [\[EC2.171\] Bei EC2 VPN-Verbindungen sollte die Protokollierung aktiviert sein](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[EC2.174\] EC2 DHCP-Optionssätze sollten mit Tags versehen werden](#)
- [\[EC2.175\] EC2 Startvorlagen sollten mit Tags versehen sein](#)
- [\[EC2.176\] EC2 Präfixlisten sollten mit Tags versehen werden](#)
- [\[EC2.177\] EC2 Traffic Mirror-Sitzungen sollten mit Tags versehen werden](#)
- [\[EC2.178\] Filter für EC2 Verkehrsspiegel sollten mit Tags versehen werden](#)
- [\[EC2.179\] EC2 Traffic-Spiegel-Ziele sollten markiert werden](#)
- [\[EC2.180\] Bei EC2 Netzwerkschnittstellen sollte die source/destination Überprüfung aktiviert sein](#)
- [\[ECR.1\] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein](#)
- [\[ECR.4\] Öffentliche ECR-Repositoryn sollten markiert werden](#)
- [\[ECS.13\] ECS-Services sollten markiert werden](#)
- [\[ECS.15\] ECS-Aufgabendefinitionen sollten mit Tags versehen werden](#)
- [\[EFS.6\] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden](#)
- [\[EKS.3\] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden](#)

- [\[EKS.6\] EKS-Cluster sollten markiert werden](#)
- [\[EKS.7\] Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden](#)
- [\[ELB.2\] Classic Load Balancer mit SSL/HTTPS Listnern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager](#)
- [\[ELB.16\] Application Load Balancers sollten mit einer Web-ACL verknüpft sein AWS WAF](#)
- [\[ELB.17\] Anwendungs- und Netzwerk-Load-Balancer mit Listnern sollten die empfohlenen Sicherheitsrichtlinien verwenden](#)
- [Bei \[ElastiCache.1\] ElastiCache \(Redis OSS\) -Clustern sollten automatische Backups aktiviert sein](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk sollte Logs streamen nach CloudWatch](#)
- [\[EMR.2\] Die Amazon EMR-Einstellung zum Blockieren des öffentlichen Zugriffs sollte aktiviert sein](#)
- [\[EMR.3\] Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden](#)
- [\[EMR.4\] Amazon EMR-Sicherheitskonfigurationen sollten bei der Übertragung verschlüsselt werden](#)
- [\[ES.4\] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein](#)
- [\[EventBridge.4\] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[FSx.1\] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden](#)
- [\[FSx.2\] FSx für Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden](#)
- [\[FSx.5\] FSx für Windows-Dateiserver sollten für die Multi-AZ-Bereitstellung konfiguriert sein](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[GuardDuty.3\] GuardDuty IPSets sollte markiert werden](#)
- [\[GuardDuty.4\] GuardDuty Detektoren sollten markiert werden](#)
- [\[GuardDuty.5\] GuardDuty EKS Audit Log Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.6\] GuardDuty Lambda Protection sollte aktiviert sein](#)
- [\[GuardDuty.7\] GuardDuty EKS Runtime Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.8\] Der GuardDuty Malware-Schutz für EC2 sollte aktiviert sein](#)

- [\[GuardDuty.9\] Der GuardDuty RDS-Schutz sollte aktiviert sein](#)
- [\[GuardDuty.10\] Der GuardDuty S3-Schutz sollte aktiviert sein](#)
- [\[GuardDuty.11\] GuardDuty Runtime Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.12\] GuardDuty ECS Runtime Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.13\] GuardDuty EC2 Runtime Monitoring sollte aktiviert sein](#)
- [\[IAM.6\] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.](#)
- [\[IAM.9\] MFA sollte für den Root-Benutzer aktiviert sein](#)
- [\[IAM.21\] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen](#)
- [\[IAM.23\] IAM Access Analyzer-Analysen sollten markiert werden](#)
- [\[IAM.24\] IAM-Rollen sollten mit Tags versehen werden](#)
- [\[IAM.25\] IAM-Benutzer sollten markiert werden](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[IAM.27\] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloud ShellFullAccess](#)
- [\[IAM.28\] Der externe Zugriffsanalysator für IAM Access Analyzer sollte aktiviert sein](#)
- [\[Inspector.1\] Das EC2 Scannen mit Amazon Inspector sollte aktiviert sein](#)
- [\[Inspector.2\] Das Amazon Inspector ECR-Scannen sollte aktiviert sein](#)
- [\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)
- [\[Inspector.4\] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein](#)
- [\[IoT Events .1\] AWS IoT-Events-Eingaben sollten markiert werden](#)
- [\[IoT Events .2\] AWS IoT-Ereignisdetektormodelle sollten markiert werden](#)
- [\[IoT Events .3\] Alarmmodelle für AWS IoT Events sollten markiert werden](#)
- [\[IoT Site Wise.1\] AWS SiteWise IoT-Asset-Modelle sollten markiert werden](#)
- [\[IoT Site Wise.2\] AWS SiteWise IoT-Dashboards sollten markiert werden](#)
- [\[IoT Site Wise.3\] AWS SiteWise IoT-Gateways sollten markiert werden](#)
- [\[IoT Site Wise.4\] AWS SiteWise IoT-Portale sollten markiert werden](#)
- [\[IoT Site Wise.5\] AWS SiteWise IoT-Projekte sollten markiert werden](#)
- [\[IoT Twin Maker.1\] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden](#)
- [\[IoT Twin Maker.2\] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden](#)
- [\[IoT Twin Maker.3\] AWS TwinMaker IoT-Szenen sollten markiert werden](#)
- [\[IoT Twin Maker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)

- [\[Io TWireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[Io TWireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)
- [\[Io TWireless .3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)
- [\[Keyspaces.1\] Amazon Keyspaces Keyspaces sollten mit Tags versehen sein](#)
- [\[Macie.1\] Amazon Macie sollte aktiviert sein](#)
- [\[Macie.2\] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein](#)
- [\[MQ.2\] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch](#)
- [\[MQ.4\] Amazon MQ-Broker sollten markiert werden](#)
- [\[MSK.3\] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden](#)
- [\[MSK.5\] Bei MSK-Konnektoren sollte die Protokollierung aktiviert sein](#)
- [\[Neptune.1\] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.2\] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)
- [\[Neptune.3\] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein](#)
- [\[Neptune.4\] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[Neptune.5\] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein](#)
- [\[Neptune.6\] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.7\] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein](#)
- [\[Neptune.8\] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren](#)
- [\[Neptune.9\] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden](#)
- [\[NetworkFirewall.1\] Network firewalls sollten über mehrere Availability Zones hinweg bereitgestellt werden](#)
- [\[NetworkFirewall.2\] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein](#)
- [\[NetworkFirewall.3\] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet haben](#)
- [\[NetworkFirewall.4\] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ sein.](#)
- [\[NetworkFirewall.5\] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ sein.](#)

- [\[NetworkFirewall.6\] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein](#)
- [\[NetworkFirewall.7\] Netzwerk-Firewall-Firewalls sollten markiert werden](#)
- [\[NetworkFirewall.9\] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein](#)
- [\[NetworkFirewall.10\] Bei Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein](#)
- [Bei \[Opensearch.1\] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein](#)
- [\[Opensearch.2\] OpenSearch -Domains sollten nicht öffentlich zugänglich sein](#)
- [\[Opensearch.3\] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden](#)
- [Die Protokollierung von \[Opensearch.4\] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein](#)
- [Für \[Opensearch.5\] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein](#)
- [\[Opensearch.6\] OpenSearch Domains sollten mindestens drei Datenknoten haben](#)
- [Für \[Opensearch.7\] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein](#)
- [\[Opensearch.8\] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden](#)
- [\[Opensearch.11\] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben](#)
- [\[PCA.1\] AWS Private CA Root-Zertifizierungsstelle sollte deaktiviert sein](#)
- [\[PCA.2\] AWS Private CA-Zertifizierungsstellen sollten gekennzeichnet werden](#)
- [\[RDS.7\] Bei RDS-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[RDS.10\] Die IAM-Authentifizierung sollte für RDS-Instances konfiguriert werden](#)
- [\[RDS.12\] Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden](#)
- [\[RDS.13\] Automatische RDS-Upgrades für Nebenversionen sollten aktiviert sein](#)
- [\[RDS.14\] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein](#)
- [\[RDS.15\] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden](#)
- [\[RDS.16\] Aurora-DB-Cluster sollten so konfiguriert sein, dass sie Tags in DB-Snapshots kopieren](#)
- [\[RDS.24\] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden](#)
- [\[RDS.25\] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden](#)

- [\[RDS.26\] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden](#)
- [\[RDS.27\] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[RDS.28\] RDS-DB-Cluster sollten markiert werden](#)
- [\[RDS.29\] RDS-DB-Cluster-Snapshots sollten markiert werden](#)
- [\[RDS.30\] RDS-DB-Instances sollten markiert werden](#)
- [\[RDS.31\] RDS-DB-Sicherheitsgruppen sollten markiert werden](#)
- [\[RDS.32\] RDS-DB-Snapshots sollten markiert werden](#)
- [\[RDS.33\] RDS-DB-Subnetzgruppen sollten markiert werden](#)
- [\[RDS.34\] Aurora MySQL-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)
- [\[RDS.35\] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein](#)
- [\[RDS.37\] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[RDS.42\] RDS für MariaDB-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[RDS.44\] RDS für MariaDB-DB-Instances sollte bei der Übertragung verschlüsselt werden](#)
- [\[RDS.45\] Bei Aurora MySQL-DB-Clustern sollte die Audit-Protokollierung aktiviert sein](#)
- [\[Redshift.10\] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[Redshift.14\] Redshift-Cluster-Subnetzgruppen sollten markiert werden](#)
- [\[Redshift.15\] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen](#)
- [\[Redshift.17\] Redshift-Cluster-Parametergruppen sollten markiert werden](#)
- [\[RedshiftServerless.1\] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden](#)
- [\[RedshiftServerless.2\] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein](#)
- [\[RedshiftServerless.3\] Serverlose Redshift-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.22\] S3-Allzweck-Buckets sollten Schreibereignisse auf Objektebene protokollieren](#)
- [\[S3.23\] S3-Allzweck-Buckets sollten Leseereignisse auf Objektebene protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)

- [\[SageMaker.1\] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben](#)
- [\[SageMaker.4\] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein](#)
- [\[SageMaker.5\] SageMaker Modelle sollten eingehenden Datenverkehr blockieren](#)
- [\[SageMaker.6\] SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden](#)
- [\[SageMaker.7\] SageMaker Bilder sollten mit Tags versehen werden](#)
- [\[SES.1\] SES-Kontaktlisten sollten mit Tags versehen werden](#)
- [\[SES.2\] SES-Konfigurationssätze sollten mit Tags versehen werden](#)
- [\[ServiceCatalog.1\] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden](#)
- [\[SSM.5\] SSM-Dokumente sollten mit Tags versehen werden](#)
- [\[SSM.6\] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[Transfer.2\] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden](#)
- [\[Transfer.4\] Transfer Family Familienverträge sollten gekennzeichnet werden](#)
- [\[Transfer.5\] Transfer Family Familienzertifikate sollten gekennzeichnet sein](#)
- [\[Transfer.6\] Steckverbinder der Transfer-Familie sollten gekennzeichnet sein](#)
- [\[Transfer.7\] Familienprofile sollten mit Tags versehen werden](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.3\] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WorkSpaces.1\] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden](#)
- [\[WorkSpaces.2\] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden](#)

China (Ningxia)

Die folgenden Steuerelemente werden in der Region China (Ningxia) nicht unterstützt.

- [\[ACM.1\] Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden](#)
- [\[ACM.2\] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden](#)
- [\[Account.2\] AWS-Konten sollte Teil einer Organisation sein AWS Organizations](#)
- [\[APIGateway.2\] API Gateway REST API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden](#)
- [\[Amplify.1\] Amplify-Apps sollten markiert werden](#)
- [\[Amplify.2\] Amplify-Zweige sollten markiert werden](#)
- [\[AppConfig.1\] AWS AppConfig Anwendungen sollten markiert werden](#)
- [\[AppConfig.2\] AWS AppConfig Konfigurationsprofile sollten mit Tags versehen werden](#)
- [\[AppConfig.3\] AWS AppConfig Umgebungen sollten markiert werden](#)
- [\[AppConfig.4\] AWS AppConfig Erweiterungszuordnungen sollten markiert werden](#)
- [\[AppFlow.1\] AppFlow Amazon-Datenflüsse sollten mit Tags versehen werden](#)
- [\[AppRunner.1\] App Runner-Dienste sollten markiert sein](#)
- [\[AppRunner.2\] App Runner VPC-Konnektoren sollten markiert sein](#)
- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [\[AutoScaling.10\] EC2 Auto Scaling Scaling-Gruppen sollten markiert werden](#)
- [\[Backup.1\] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein](#)
- [\[Backup.4\] AWS Backup Berichtspläne sollten markiert werden](#)
- [\[Batch.1\] Warteschlangen für Batch-Jobs sollten markiert werden](#)
- [\[Batch.2\] Richtlinien für die Batch-Planung sollten gekennzeichnet sein](#)
- [\[Batch.3\] Batch-Computing-Umgebungen sollten markiert werden](#)
- [\[Batch.4\] Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)

- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[CloudTrail.10\] Event-Datenspeicher in CloudTrail Lake sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys](#)
- [\[CodeArtifact.1\] CodeArtifact Repositorien sollten mit Tags versehen werden](#)
- [\[CodeGuruProfiler.1\] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden](#)
- [\[CodeGuruReviewer.1\] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden](#)
- [\[Cognito.1\] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein](#)
- [\[Cognito.2\] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen](#)
- [\[Connect.1\] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden](#)
- [\[Connect.2\] Für Amazon Connect Connect-Instances sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[DataFirehose.1\] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden](#)
- [\[DataSync.2\] DataSync Aufgaben sollten mit Tags versehen werden](#)
- [\[Detective.1\] Verhaltensdiagramme von Detektiven sollten markiert werden](#)
- [\[DMS.4\] DMS-Replikationsinstanzen sollten markiert werden](#)
- [\[DMS.5\] Subnetzgruppen für die DMS-Replikation sollten markiert werden](#)
- [\[DMS.10\] Bei DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein](#)

- [\[DMS.11\] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein](#)
- [\[DMS.12\] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein](#)
- [\[DocumentDB.3\] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein](#)
- [\[DynamoDB.3\] DynamoDB Accelerator \(DAX\) -Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DynamoDB.4\] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein](#)
- [\[DynamoDB.7\] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[EC2.15\] EC2 Amazon-Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen](#)
- [\[EC2.16\] Ungenutzte Network Access Control Lists sollten entfernt werden](#)
- [\[EC2.20\] Beide VPN-Tunnel für eine AWS Site-to-Site VPN-Verbindung sollten aktiv sein](#)
- [\[EC2.22\] Ungenutzte EC2 Amazon-Sicherheitsgruppen sollten entfernt werden](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways sollte VPC-Anhangsanfragen nicht automatisch akzeptieren](#)
- [\[EC2.24\] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden](#)
- [\[EC2.28\] EBS-Volumes sollten durch einen Backup-Plan abgedeckt sein](#)
- [\[EC2.33\] EC2 Transit-Gateway-Anhänge sollten mit Tags versehen werden](#)
- [\[EC2.34\] Die Routentabellen für EC2 Transit-Gateways sollten mit Tags versehen werden](#)
- [\[EC2.35\] EC2 Netzwerkschnittstellen sollten markiert werden](#)
- [\[EC2.36\] EC2 Kunden-Gateways sollten mit Tags versehen werden](#)
- [\[EC2.40\] EC2 NAT-Gateways sollten markiert werden](#)
- [\[EC2.41\] Das EC2 Netzwerk ACLs sollte markiert sein](#)
- [\[EC2.42\] EC2 Routing-Tabellen sollten mit Tags versehen werden](#)
- [\[EC2.43\] EC2 Sicherheitsgruppen sollten markiert werden](#)
- [\[EC2.44\] EC2 Subnetze sollten markiert werden](#)
- [\[EC2.46\] Amazon VPCs sollte markiert werden](#)
- [\[EC2.47\] Amazon VPC Endpoint Services sollten markiert werden](#)
- [\[EC2.48\] Amazon VPC-Flow-Logs sollten mit Tags versehen werden](#)
- [\[EC2.49\] Amazon VPC-Peering-Verbindungen sollten markiert werden](#)
- [\[EC2.50\] EC2 VPN-Gateways sollten markiert werden](#)

- [\[EC2.51\] EC2 Client-VPN-Endpunkte sollten die Client-Verbindungsprotokollierung aktiviert haben](#)
- [\[EC2.58\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert sein](#)
- [\[EC2.60\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden](#)
- [\[EC2.171\] Bei EC2 VPN-Verbindungen sollte die Protokollierung aktiviert sein](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[EC2.174\] EC2 DHCP-Optionssätze sollten mit Tags versehen werden](#)
- [\[EC2.175\] EC2 Startvorlagen sollten mit Tags versehen sein](#)
- [\[EC2.176\] EC2 Präfixlisten sollten mit Tags versehen werden](#)
- [\[EC2.177\] EC2 Traffic Mirror-Sitzungen sollten mit Tags versehen werden](#)
- [\[EC2.178\] Filter für EC2 Verkehrsspiegel sollten mit Tags versehen werden](#)
- [\[EC2.179\] EC2 Traffic-Spiegel-Ziele sollten markiert werden](#)
- [\[ECR.1\] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein](#)
- [\[ECR.4\] Öffentliche ECR-Repositoryn sollten markiert werden](#)
- [\[ECS.13\] ECS-Services sollten markiert werden](#)
- [\[ECS.15\] ECS-Aufgabendefinitionen sollten mit Tags versehen werden](#)
- [\[EFS.3\] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen](#)
- [\[EFS.4\] EFS-Zugangspunkte sollten eine Benutzeridentität erzwingen](#)
- [\[EFS.6\] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden](#)
- [\[EKS.3\] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden](#)
- [\[EKS.6\] EKS-Cluster sollten markiert werden](#)
- [\[EKS.7\] Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden](#)
- [\[ELB.2\] Classic Load Balancer mit SSL/HTTPS Listnern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager](#)
- [\[ELB.16\] Application Load Balancers sollten mit einer Web-ACL verknüpft sein AWS WAF](#)
- [\[ELB.17\] Anwendungs- und Netzwerk-Load-Balancer mit Listnern sollten die empfohlenen Sicherheitsrichtlinien verwenden](#)
- [Bei \[ElastiCache.1\] ElastiCache \(Redis OSS\) -Clustern sollten automatische Backups aktiviert sein](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk sollte Logs streamen nach CloudWatch](#)

- [\[EMR.2\] Die Amazon EMR-Einstellung zum Blockieren des öffentlichen Zugriffs sollte aktiviert sein](#)
- [\[EMR.3\] Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden](#)
- [\[EMR.4\] Amazon EMR-Sicherheitskonfigurationen sollten bei der Übertragung verschlüsselt werden](#)
- [\[ES.4\] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein](#)
- [\[EventBridge.4\] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[FSx.1\] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden](#)
- [\[FSx.2\] FSx für Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden](#)
- [\[FSx.5\] FSx für Windows-Dateiserver sollten für die Multi-AZ-Bereitstellung konfiguriert sein](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[Glue.3\] Transformationen für AWS Glue maschinelles Lernen sollten im Ruhezustand verschlüsselt werden](#)
- [\[GuardDuty.3\] GuardDuty IPSets sollte markiert werden](#)
- [\[GuardDuty.4\] GuardDuty Detektoren sollten markiert werden](#)
- [\[GuardDuty.5\] GuardDuty EKS Audit Log Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.6\] GuardDuty Lambda Protection sollte aktiviert sein](#)
- [\[GuardDuty.7\] GuardDuty EKS Runtime Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.8\] Der GuardDuty Malware-Schutz für EC2 sollte aktiviert sein](#)
- [\[GuardDuty.9\] Der GuardDuty RDS-Schutz sollte aktiviert sein](#)
- [\[GuardDuty.10\] Der GuardDuty S3-Schutz sollte aktiviert sein](#)
- [\[GuardDuty.11\] GuardDuty Runtime Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.12\] GuardDuty ECS Runtime Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.13\] GuardDuty EC2 Runtime Monitoring sollte aktiviert sein](#)
- [\[IAM.6\] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.](#)
- [\[IAM.9\] MFA sollte für den Root-Benutzer aktiviert sein](#)

- [\[IAM.21\] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen](#)
- [\[IAM.23\] IAM Access Analyzer-Analyzer sollten markiert werden](#)
- [\[IAM.24\] IAM-Rollen sollten mit Tags versehen werden](#)
- [\[IAM.25\] IAM-Benutzer sollten markiert werden](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[IAM.27\] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWS Cloud Shell FullAccess](#)
- [\[IAM.28\] Der externe Zugriffsanalysator für IAM Access Analyzer sollte aktiviert sein](#)
- [\[Inspector.1\] Das EC2 Scannen mit Amazon Inspector sollte aktiviert sein](#)
- [\[Inspector.2\] Das Amazon Inspector ECR-Scannen sollte aktiviert sein](#)
- [\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)
- [\[Inspector.4\] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein](#)
- [\[IoT Events .1\] AWS IoT-Events-Eingaben sollten markiert werden](#)
- [\[IoT Events .2\] AWS IoT-Ereignisdetektormodelle sollten markiert werden](#)
- [\[IoT Events .3\] Alarmmodelle für AWS IoT Events sollten markiert werden](#)
- [\[IoT Site Wise.1\] AWS SiteWise IoT-Asset-Modelle sollten markiert werden](#)
- [\[IoT Site Wise.2\] AWS SiteWise IoT-Dashboards sollten markiert werden](#)
- [\[IoT Site Wise.3\] AWS SiteWise IoT-Gateways sollten markiert werden](#)
- [\[IoT Site Wise.4\] AWS SiteWise IoT-Portale sollten markiert werden](#)
- [\[IoT Site Wise.5\] AWS SiteWise IoT-Projekte sollten markiert werden](#)
- [\[IoT Twin Maker.1\] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden](#)
- [\[IoT Twin Maker.2\] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden](#)
- [\[IoT Twin Maker.3\] AWS TwinMaker IoT-Szenen sollten markiert werden](#)
- [\[IoT Twin Maker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[IoT Wireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[IoT Wireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)
- [\[IoT Wireless .3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)

- [\[Keyspaces.1\] Amazon Keyspaces Keyspaces sollten mit Tags versehen sein](#)
- [\[Lambda.1\] Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten](#)
- [\[Lambda.2\] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden](#)
- [\[Lambda.3\] Lambda-Funktionen sollten sich in einer VPC befinden](#)
- [\[Lambda.5\] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren](#)
- [\[Lambda.6\] Lambda-Funktionen sollten markiert werden](#)
- [\[Lambda.7\] Bei Lambda-Funktionen sollte aktives Tracing aktiviert sein AWS X-Ray](#)
- [\[Macie.1\] Amazon Macie sollte aktiviert sein](#)
- [\[Macie.2\] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein](#)
- [\[MQ.2\] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch](#)
- [\[MQ.4\] Amazon MQ-Broker sollten markiert werden](#)
- [\[MSK.3\] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden](#)
- [\[MSK.5\] Bei MSK-Konnektoren sollte die Protokollierung aktiviert sein](#)
- [\[Neptune.3\] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein](#)
- [\[NetworkFirewall.1\] Network firewalls sollten über mehrere Availability Zones hinweg bereitgestellt werden](#)
- [\[NetworkFirewall.2\] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein](#)
- [\[NetworkFirewall.3\] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet haben](#)
- [\[NetworkFirewall.4\] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ sein.](#)
- [\[NetworkFirewall.5\] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ sein.](#)
- [\[NetworkFirewall.6\] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein](#)
- [\[NetworkFirewall.7\] Netzwerk-Firewall-Firewalls sollten markiert werden](#)
- [\[NetworkFirewall.9\] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein](#)
- [\[NetworkFirewall.10\] Bei Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein](#)
- [Bei \[Opensearch.1\] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein](#)
- [\[Opensearch.2\] OpenSearch -Domains sollten nicht öffentlich zugänglich sein](#)

- [\[Opensearch.3\] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden](#)
- [Die Protokollierung von \[Opensearch.4\] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein](#)
- [Für \[Opensearch.5\] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein](#)
- [\[Opensearch.6\] OpenSearch Domains sollten mindestens drei Datenknoten haben](#)
- [Für \[Opensearch.7\] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein](#)
- [\[Opensearch.8\] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden](#)
- [\[Opensearch.11\] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben](#)
- [\[PCA.1\] AWS Private CA Root-Zertifizierungsstelle sollte deaktiviert sein](#)
- [\[PCA.2\] AWS Private CA-Zertifizierungsstellen sollten gekennzeichnet werden](#)
- [\[RDS.7\] Bei RDS-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[RDS.9\] RDS-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[RDS.10\] Die IAM-Authentifizierung sollte für RDS-Instances konfiguriert werden](#)
- [\[RDS.12\] Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden](#)
- [\[RDS.13\] Automatische RDS-Upgrades für Nebenversionen sollten aktiviert sein](#)
- [\[RDS.14\] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein](#)
- [\[RDS.15\] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden](#)
- [\[RDS.24\] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden](#)
- [\[RDS.25\] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden](#)
- [\[RDS.26\] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden](#)
- [\[RDS.28\] RDS-DB-Cluster sollten markiert werden](#)
- [\[RDS.29\] RDS-DB-Cluster-Snapshots sollten markiert werden](#)
- [\[RDS.30\] RDS-DB-Instances sollten markiert werden](#)
- [\[RDS.31\] RDS-DB-Sicherheitsgruppen sollten markiert werden](#)
- [\[RDS.32\] RDS-DB-Snapshots sollten markiert werden](#)
- [\[RDS.33\] RDS-DB-Subnetzgruppen sollten markiert werden](#)
- [\[RDS.34\] Aurora MySQL-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)

- [\[RDS.35\] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein](#)
- [\[RDS.42\] RDS für MariaDB-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[RDS.44\] RDS für MariaDB-DB-Instances sollte bei der Übertragung verschlüsselt werden](#)
- [\[RDS.45\] Bei Aurora MySQL-DB-Clustern sollte die Audit-Protokollierung aktiviert sein](#)
- [\[Redshift.10\] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[Redshift.14\] Redshift-Cluster-Subnetzgruppen sollten markiert werden](#)
- [\[Redshift.15\] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen](#)
- [\[Redshift.17\] Redshift-Cluster-Parametergruppen sollten markiert werden](#)
- [\[RedshiftServerless.1\] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden](#)
- [\[RedshiftServerless.2\] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein](#)
- [\[RedshiftServerless.3\] Serverlose Redshift-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)
- [\[SageMaker.1\] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben](#)
- [\[SageMaker.4\] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein](#)
- [\[SageMaker.5\] SageMaker Modelle sollten eingehenden Datenverkehr blockieren](#)
- [\[SageMaker.6\] SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden](#)
- [\[SageMaker.7\] SageMaker Bilder sollten mit Tags versehen werden](#)
- [\[ServiceCatalog.1\] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden](#)
- [\[SSM.5\] SSM-Dokumente sollten mit Tags versehen werden](#)
- [\[SSM.7\] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein](#)
- [\[StepFunctions.2\] Die Aktivitäten von Step Functions sollten mit Tags versehen werden](#)

- [\[Transfer.2\] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden](#)
- [\[Transfer.4\] Transfer Family Familienverträge sollten gekennzeichnet werden](#)
- [\[Transfer.5\] Transfer Family Familienzertifikate sollten gekennzeichnet sein](#)
- [\[Transfer.6\] Steckverbinder der Transfer-Familie sollten gekennzeichnet sein](#)
- [\[Transfer.7\] Familienprofile sollten mit Tags versehen werden](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.3\] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)

Europa (Frankfurt)

Die folgenden Steuerelemente werden in der Region Europa (Frankfurt) nicht unterstützt.

- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)

- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[ECR.4\] Öffentliche ECR-Repositoryn sollten markiert werden](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[RDS.31\] RDS-DB-Sicherheitsgruppen sollten markiert werden](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)

Europa (Irland)

Die folgenden Steuerelemente werden in der Region Europa (Irland) nicht unterstützt.

- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)

- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[Connect.1\] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden](#)
- [\[Connect.2\] Für Amazon Connect Connect-Instances sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[ECR.4\] Öffentliche ECR-Repositorien sollten markiert werden](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)

- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)

Europa (London)

Die folgenden Steuerelemente werden in der Region Europa (London) nicht unterstützt.

- [\[AppRunner.2\] App Runner VPC-Konnektoren sollten markiert sein](#)
- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[EC2.24\] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[ECR.4\] Öffentliche ECR-Repositoryn sollten markiert werden](#)

- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[IoT Site Wise.1\] AWS SiteWise IoT-Asset-Modelle sollten markiert werden](#)
- [\[IoT Site Wise.2\] AWS SiteWise IoT-Dashboards sollten markiert werden](#)
- [\[IoT Site Wise.3\] AWS SiteWise IoT-Gateways sollten markiert werden](#)
- [\[IoT Site Wise.4\] AWS SiteWise IoT-Portale sollten markiert werden](#)
- [\[IoT Site Wise.5\] AWS SiteWise IoT-Projekte sollten markiert werden](#)
- [\[IoT Twin Maker.1\] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden](#)
- [\[IoT Twin Maker.2\] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden](#)
- [\[IoT Twin Maker.3\] AWS TwinMaker IoT-Szenen sollten markiert werden](#)
- [\[IoT Twin Maker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[IoT Wireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[IoT Wireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)
- [\[IoT Wireless .3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)
- [\[RDS.31\] RDS-DB-Sicherheitsgruppen sollten markiert werden](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)

- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)

Europa (Milan)

Die folgenden Steuerelemente werden in der Region Europa (Mailand) nicht unterstützt.

- [\[AppFlow.1\] AppFlow Amazon-Datenflüsse sollten mit Tags versehen werden](#)
- [\[AppRunner.1\] App Runner-Dienste sollten markiert sein](#)
- [\[AppRunner.2\] App Runner VPC-Konnektoren sollten markiert sein](#)
- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[CodeGuruProfiler.1\] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden](#)
- [\[CodeGuruReviewer.1\] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden](#)

- [\[Connect.1\] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden](#)
- [\[Connect.2\] Für Amazon Connect Connect-Instances sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[DMS.10\] Bei DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein](#)
- [\[DynamoDB.3\] DynamoDB Accelerator \(DAX\) -Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DynamoDB.7\] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[EC2.4\] Gestoppte EC2 Instances sollten nach einem bestimmten Zeitraum entfernt werden](#)
- [\[EC2.8\] EC2 Instances sollten Instance Metadata Service Version 2 \(\) verwenden IMDSv2](#)
- [\[EC2.14\] Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 oder: :/0 auf Port 3389 zulassen](#)
- [\[EC2.24\] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden](#)
- [\[EC2.58\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert sein](#)
- [\[EC2.60\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[EC2.177\] EC2 Traffic Mirror-Sitzungen sollten mit Tags versehen werden](#)
- [\[ECR.4\] Öffentliche ECR-Repositoryn sollten markiert werden](#)
- [\[ELB.2\] Classic Load Balancer mit SSL/HTTPS Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager](#)
- [\[EventBridge.4\] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[IAM.18\] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS -Support](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)

- [\[IoT.1\] AWS IoT Device Defender Sicherheitsprofile sollten markiert werden](#)
- [\[IoT.2\] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden](#)
- [\[IoT.3\] AWS IoT Core -Dimensionen sollten markiert werden](#)
- [\[IoT.4\] AWS IoT Core Autorisierer sollten markiert werden](#)
- [\[IoT.5\] AWS IoT Core Rollenalias sollten markiert werden](#)
- [\[IoT.6\] AWS IoT Core Richtlinien sollten markiert werden](#)
- [\[IoT Events .1\] AWS IoT-Events-Eingaben sollten markiert werden](#)
- [\[IoT Events .2\] AWS IoT-Ereignisdetektormodelle sollten markiert werden](#)
- [\[IoT Events .3\] Alarmmodelle für AWS IoT Events sollten markiert werden](#)
- [\[IoT Site Wise.1\] AWS SiteWise IoT-Asset-Modelle sollten markiert werden](#)
- [\[IoT Site Wise.2\] AWS SiteWise IoT-Dashboards sollten markiert werden](#)
- [\[IoT Site Wise.3\] AWS SiteWise IoT-Gateways sollten markiert werden](#)
- [\[IoT Site Wise.4\] AWS SiteWise IoT-Portale sollten markiert werden](#)
- [\[IoT Site Wise.5\] AWS SiteWise IoT-Projekte sollten markiert werden](#)
- [\[IoT TTwin Maker.1\] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden](#)
- [\[IoT TTwin Maker.2\] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden](#)
- [\[IoT TTwin Maker.3\] AWS TwinMaker IoT-Szenen sollten markiert werden](#)
- [\[IoT TTwin Maker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[IoT TWireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[IoT TWireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)
- [\[IoT TWireless .3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)
- [\[Keyspaces.1\] Amazon Keyspaces Keyspaces sollten mit Tags versehen sein](#)
- [\[MSK.3\] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden](#)
- [\[MSK.5\] Bei MSK-Konnektoren sollte die Protokollierung aktiviert sein](#)
- [\[Neptune.1\] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.2\] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)
- [\[Neptune.3\] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein](#)

- [\[Neptune.4\] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[Neptune.5\] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein](#)
- [\[Neptune.6\] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.7\] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein](#)
- [\[Neptune.8\] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren](#)
- [\[Neptune.9\] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden](#)
- [\[RDS.1\] Der RDS-Snapshot sollte privat sein](#)
- [\[RDS.14\] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein](#)
- [\[RDS.31\] RDS-DB-Sicherheitsgruppen sollten markiert werden](#)
- [\[RedshiftServerless.1\] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden](#)
- [\[RedshiftServerless.2\] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein](#)
- [\[RedshiftServerless.3\] Serverlose Redshift-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten](#)
- [\[RedshiftServerless.4\] Serverlose Redshift-Namespace sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys](#)
- [\[RedshiftServerless.5\] Redshift Serverless-Namespace sollten nicht den Standard-Admin-Benutzernamen verwenden](#)
- [\[RedshiftServerless.6\] Redshift Serverless Namespace sollten Protokolle in Logs exportieren CloudWatch](#)
- [\[RedshiftServerless.7\] Redshift Serverless-Namespace sollten nicht den Standard-Datenbanknamen verwenden](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)
- [\[SSM.2\] Von Systems Manager verwaltete EC2 Amazon-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben](#)
- [\[SSM.3\] Von Systems Manager verwaltete EC2 Amazon-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)

- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WorkSpaces.1\] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden](#)
- [\[WorkSpaces.2\] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden](#)

Europa (Paris)

Die folgenden Steuerelemente werden in der Region Europa (Paris) nicht unterstützt.

- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[CodeGuruProfiler.1\] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden](#)

- [\[CodeGuruReviewer.1\] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden](#)
- [\[Connect.1\] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden](#)
- [\[Connect.2\] Für Amazon Connect Connect-Instances sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[EC2.24\] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[ECR.4\] Öffentliche ECR-Repositorien sollten markiert werden](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[FSx.5\] FSx für Windows-Dateiserver sollten für die Multi-AZ-Bereitstellung konfiguriert sein](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)
- [\[IoTEvents .1\] AWS IoT-Events-Eingaben sollten markiert werden](#)
- [\[IoTEvents .2\] AWS IoT-Ereignisdetektormodelle sollten markiert werden](#)
- [\[IoTEvents .3\] Alarmmodelle für AWS IoT Events sollten markiert werden](#)
- [\[IoTSiteWise.1\] AWS SiteWise IoT-Asset-Modelle sollten markiert werden](#)
- [\[IoTSiteWise.2\] AWS SiteWise IoT-Dashboards sollten markiert werden](#)
- [\[IoTSiteWise.3\] AWS SiteWise IoT-Gateways sollten markiert werden](#)
- [\[IoTSiteWise.4\] AWS SiteWise IoT-Portale sollten markiert werden](#)
- [\[IoTSiteWise.5\] AWS SiteWise IoT-Projekte sollten markiert werden](#)
- [\[IoT Twin Maker.1\] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden](#)
- [\[IoT Twin Maker.2\] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden](#)
- [\[IoT Twin Maker.3\] AWS TwinMaker IoT-Szenen sollten markiert werden](#)
- [\[IoT Twin Maker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[IoT Wireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[IoT Wireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)

- [\[Io TWireless .3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)
- [\[RDS.31\] RDS-DB-Sicherheitsgruppen sollten markiert werden](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WorkSpaces.1\] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden](#)
- [\[WorkSpaces.2\] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden](#)

Europa (Spain)

Die folgenden Steuerelemente werden in der Region Europa (Spanien) nicht unterstützt.

- [\[Account.2\] AWS-Konten sollte Teil einer Organisation sein AWS Organizations](#)
- [\[APIGateway.8\] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben](#)
- [\[APIGateway.9\] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein](#)
- [\[Amplify.1\] Amplify-Apps sollten markiert werden](#)
- [\[Amplify.2\] Amplify-Zweige sollten markiert werden](#)
- [\[AppConfig.1\] AWS AppConfig Anwendungen sollten markiert werden](#)
- [\[AppConfig.2\] AWS AppConfig Konfigurationsprofile sollten mit Tags versehen werden](#)
- [\[AppConfig.3\] AWS AppConfig Umgebungen sollten markiert werden](#)
- [\[AppFlow.1\] AppFlow Amazon-Datenflüsse sollten mit Tags versehen werden](#)
- [\[AppRunner.1\] App Runner-Dienste sollten markiert sein](#)

- [\[AppRunner.2\] App Runner VPC-Konnektoren sollten markiert sein](#)
- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [\[Backup.1\] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein](#)
- [\[Backup.4\] AWS Backup Berichtspläne sollten markiert werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[CodeArtifact.1\] CodeArtifact Repositorien sollten mit Tags versehen werden](#)
- [\[CodeGuruProfiler.1\] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden](#)
- [\[CodeGuruReviewer.1\] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden](#)
- [\[Cognito.1\] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein](#)
- [\[Cognito.2\] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen](#)
- [\[Connect.1\] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden](#)

- [\[Connect.2\] Für Amazon Connect Connect-Instances sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[Detective.1\] Verhaltensdiagramme von Detektiven sollten markiert werden](#)
- [\[DMS.2\] DMS-Zertifikate sollten gekennzeichnet sein](#)
- [\[DMS.3\] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden](#)
- [\[DMS.4\] DMS-Replikationsinstanzen sollten markiert werden](#)
- [\[DMS.5\] Subnetzgruppen für die DMS-Replikation sollten markiert werden](#)
- [\[DMS.6\] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein](#)
- [\[DMS.7\] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.8\] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.9\] DMS-Endpunkte sollten SSL verwenden](#)
- [\[DMS.10\] Bei DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein](#)
- [\[DMS.11\] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein](#)
- [\[DMS.12\] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein](#)
- [\[DocumentDB.1\] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DocumentDB.2\] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen](#)
- [\[DocumentDB.3\] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein](#)
- [\[DocumentDB.4\] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch](#)
- [\[DocumentDB.5\] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[DocumentDB.6\] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[DynamoDB.3\] DynamoDB Accelerator \(DAX\) -Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DynamoDB.4\] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein](#)
- [\[DynamoDB.7\] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden](#)

- [\[EC2.1\] Amazon EBS-Snapshots sollten nicht öffentlich wiederherstellbar sein](#)
- [\[EC2.4\] Gestoppte EC2 Instances sollten nach einem bestimmten Zeitraum entfernt werden](#)
- [\[EC2.8\] EC2 Instances sollten Instance Metadata Service Version 2 \(\) verwenden IMDSv2](#)
- [\[EC2.14\] Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 oder: :/0 auf Port 3389 zulassen](#)
- [\[EC2.22\] Ungenutzte EC2 Amazon-Sicherheitsgruppen sollten entfernt werden](#)
- [\[EC2.24\] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden](#)
- [\[EC2.25\] EC2 Amazon-Startvorlagen sollten Netzwerkschnittstellen nicht öffentlich IPs zuweisen](#)
- [\[EC2.28\] EBS-Volumes sollten durch einen Backup-Plan abgedeckt sein](#)
- [\[EC2.34\] Die Routentabellen für EC2 Transit-Gateways sollten mit Tags versehen werden](#)
- [\[EC2.40\] EC2 NAT-Gateways sollten markiert werden](#)
- [\[EC2.48\] Amazon VPC-Flow-Logs sollten mit Tags versehen werden](#)
- [\[EC2.51\] EC2 Client-VPN-Endpunkte sollten die Client-Verbindungsprotokollierung aktiviert haben](#)
- [\[EC2.58\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert sein](#)
- [\[EC2.60\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden](#)
- [\[EC2.170\] EC2 Startvorlagen sollten Instance Metadata Service Version 2 \(\) verwenden IMDSv2](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[EC2.175\] EC2 Startvorlagen sollten mit Tags versehen sein](#)
- [\[EC2.177\] EC2 Traffic Mirror-Sitzungen sollten mit Tags versehen werden](#)
- [\[EC2.179\] EC2 Traffic-Spiegel-Ziele sollten markiert werden](#)
- [\[EC2.180\] Bei EC2 Netzwerkschnittstellen sollte die source/destination Überprüfung aktiviert sein](#)
- [\[ECR.4\] Öffentliche ECR-Repositoryn sollten markiert werden](#)
- [\[EFS.1\] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS](#)
- [\[EFS.2\] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein](#)
- [\[ELB.2\] Classic Load Balancer mit SSL/HTTPS Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager](#)
- [\[ELB.14\] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden](#)

- [\[ELB.17\] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden](#)
- [\[ELB.18\] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln](#)
- [Bei \[ElastiCache.1\] ElastiCache \(Redis OSS\) -Clustern sollten automatische Backups aktiviert sein](#)
- [\[ElastiCache.6\] Für Replikationsgruppen ElastiCache \(Redis OSS\) früherer Versionen sollte Redis OSS AUTH aktiviert sein](#)
- [\[ElastiCache.7\] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden](#)
- [\[ElasticBeanstalk.1\] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben](#)
- [\[ElasticBeanstalk.2\] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk sollte Logs streamen nach CloudWatch](#)
- [\[EMR.1\] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben](#)
- [\[ES.4\] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein](#)
- [\[EventBridge.4\] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[Glue.4\] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue](#)
- [\[GuardDuty.2\] GuardDuty Filter sollten mit Tags versehen sein](#)
- [\[GuardDuty.3\] GuardDuty IPSets sollte markiert werden](#)
- [\[IAM.1\] IAM-Richtlinien sollten keine vollen „*“-Administratorrechte zulassen](#)
- [\[IAM.2\] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein](#)
- [\[IAM.3\] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden](#)
- [\[IAM.4\] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren](#)
- [\[IAM.5\] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen](#)
- [\[IAM.8\] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden](#)

- [\[IAM.18\] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS -Support](#)
- [\[IAM.19\] MFA sollte für alle IAM-Benutzer aktiviert sein](#)
- [\[IAM.21\] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen](#)
- [\[IAM.22\] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden](#)
- [\[IAM.24\] IAM-Rollen sollten mit Tags versehen werden](#)
- [\[IAM.25\] IAM-Benutzer sollten markiert werden](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[IAM.27\] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWS Cloud Shell FullAccess](#)
- [\[Inspector.1\] Das EC2 Scannen mit Amazon Inspector sollte aktiviert sein](#)
- [\[Inspector.2\] Das Amazon Inspector ECR-Scannen sollte aktiviert sein](#)
- [\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)
- [\[Inspector.4\] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein](#)
- [\[IoT.1\] AWS IoT Device Defender Sicherheitsprofile sollten markiert werden](#)
- [\[IoT.2\] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden](#)
- [\[IoT.3\] AWS IoT Core -Dimensionen sollten markiert werden](#)
- [\[IoT.4\] AWS IoT Core Autorisierer sollten markiert werden](#)
- [\[IoT.5\] AWS IoT Core Rollenalias sollten markiert werden](#)
- [\[IoT.6\] AWS IoT Core Richtlinien sollten markiert werden](#)
- [\[IoT Events .1\] AWS IoT-Events-Eingaben sollten markiert werden](#)
- [\[IoT Events .2\] AWS IoT-Ereignisdetektormodelle sollten markiert werden](#)
- [\[IoT Events .3\] Alarmmodelle für AWS IoT Events sollten markiert werden](#)
- [\[IoT Site Wise.1\] AWS SiteWise IoT-Asset-Modelle sollten markiert werden](#)
- [\[IoT Site Wise.2\] AWS SiteWise IoT-Dashboards sollten markiert werden](#)
- [\[IoT Site Wise.3\] AWS SiteWise IoT-Gateways sollten markiert werden](#)
- [\[IoT Site Wise.4\] AWS SiteWise IoT-Portale sollten markiert werden](#)
- [\[IoT Site Wise.5\] AWS SiteWise IoT-Projekte sollten markiert werden](#)
- [\[IoT Twin Maker.1\] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden](#)
- [\[IoT Twin Maker.2\] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden](#)

- [\[Io TTwin Maker.3\] AWS TwinMaker IoT-Szenen sollten markiert werden](#)
- [\[Io TTwin Maker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[Io TWireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[Io TWireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)
- [\[Io TWireless .3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)
- [\[Keyspaces.1\] Amazon Keyspaces Keyspaces sollten mit Tags versehen sein](#)
- [\[KMS.1\] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)
- [\[KMS.2\] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)
- [\[Lambda.1\] Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten](#)
- [\[Lambda.7\] Bei Lambda-Funktionen sollte aktives Tracing aktiviert sein AWS X-Ray](#)
- [\[Macie.1\] Amazon Macie sollte aktiviert sein](#)
- [\[Macie.2\] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein](#)
- [\[MQ.2\] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch](#)
- [\[MQ.3\] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein](#)
- [\[MQ.4\] Amazon MQ-Broker sollten markiert werden](#)
- [\[MQ.5\] ActiveMQ-Broker sollten den Aktiv-/Standby-Bereitstellungsmodus verwenden](#)
- [\[MQ.6\] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden](#)
- [\[MSK.3\] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden](#)
- [\[MSK.4\] Bei MSK-Clustern sollte der öffentliche Zugriff deaktiviert sein](#)
- [\[MSK.5\] Bei MSK-Konnektoren sollte die Protokollierung aktiviert sein](#)
- [\[MSK.6\] MSK-Cluster sollten den nicht authentifizierten Zugriff deaktivieren](#)
- [\[Neptune.1\] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.2\] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)
- [\[Neptune.3\] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein](#)
- [\[Neptune.4\] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein](#)

- [\[Neptune.5\] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein](#)
- [\[Neptune.6\] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.7\] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein](#)
- [\[Neptune.8\] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren](#)
- [\[Neptune.9\] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden](#)
- [Bei \[Opensearch.1\] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein](#)
- [\[Opensearch.2\] OpenSearch -Domains sollten nicht öffentlich zugänglich sein](#)
- [\[Opensearch.3\] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden](#)
- [Die Protokollierung von \[Opensearch.4\] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein](#)
- [Für \[Opensearch.5\] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein](#)
- [\[Opensearch.6\] OpenSearch Domains sollten mindestens drei Datenknoten haben](#)
- [Für \[Opensearch.7\] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein](#)
- [\[Opensearch.8\] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden](#)
- [\[Opensearch.9\] OpenSearch -Domains sollten mit Tags versehen werden](#)
- [Auf \[Opensearch.10\] OpenSearch -Domains sollte das neueste Softwareupdate installiert sein](#)
- [\[Opensearch.11\] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben](#)
- [\[RDS.1\] Der RDS-Snapshot sollte privat sein](#)
- [\[RDS.14\] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein](#)
- [\[RDS.15\] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden](#)
- [\[RDS.26\] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden](#)
- [\[RDS.31\] RDS-DB-Sicherheitsgruppen sollten markiert werden](#)
- [\[RDS.35\] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein](#)
- [\[RDS.37\] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[Redshift.10\] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[Redshift.18\] Für Redshift-Cluster sollten Multi-AZ-Bereitstellungen aktiviert sein](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)

- [\[S3.6\] Allgemeine S3-Bucket-Richtlinien sollten den Zugriff auf andere einschränken AWS-Konten](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)
- [\[SageMaker.1\] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben](#)
- [\[SageMaker.2\] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden](#)
- [\[SageMaker.3\] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben](#)
- [\[SageMaker.5\] SageMaker Modelle sollten eingehenden Datenverkehr blockieren](#)
- [\[SES.1\] SES-Kontaktlisten sollten mit Tags versehen werden](#)
- [\[SES.2\] SES-Konfigurationssätze sollten mit Tags versehen werden](#)
- [\[SQS.1\] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt werden](#)
- [\[SQS.2\] SQS-Warteschlangen sollten markiert werden](#)
- [\[SQS.3\] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen](#)
- [\[SSM.3\] Von Systems Manager verwaltete EC2 Amazon-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben](#)
- [\[SSM.6\] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[SSM.7\] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein](#)
- [\[Transfer.3\] Bei Connectoren der Transfer-Familie sollte die Protokollierung aktiviert sein](#)
- [\[Transfer.4\] Transfer Family Familienverträge sollten gekennzeichnet werden](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.3\] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WAF.10\] AWS WAF web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WorkSpaces.1\] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden](#)
- [\[WorkSpaces.2\] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden](#)

Europa (Stockholm)

Die folgenden Steuerelemente werden in der Region Europa (Stockholm) nicht unterstützt.

- [\[AppFlow.1\] AppFlow Amazon-Datenflüsse sollten mit Tags versehen werden](#)
- [\[AppRunner.1\] App Runner-Dienste sollten markiert sein](#)
- [\[AppRunner.2\] App Runner VPC-Konnektoren sollten markiert sein](#)
- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[Connect.1\] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden](#)
- [\[Connect.2\] Für Amazon Connect Connect-Instances sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[DocumentDB.1\] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden](#)

- [\[DocumentDB.2\] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen](#)
- [\[DocumentDB.3\] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein](#)
- [\[DocumentDB.4\] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch](#)
- [\[DocumentDB.5\] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[DocumentDB.6\] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[DynamoDB.3\] DynamoDB Accelerator \(DAX\) -Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DynamoDB.7\] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[EC2.24\] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[ECR.4\] Öffentliche ECR-Repositoryn sollten markiert werden](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[IoTEvents .1\] AWS IoT-Events-Eingaben sollten markiert werden](#)
- [\[IoTEvents .2\] AWS IoT-Ereignisdetektormodelle sollten markiert werden](#)
- [\[IoTEvents .3\] Alarmmodelle für AWS IoT Events sollten markiert werden](#)
- [\[IoTSiteWise.1\] AWS SiteWise IoT-Asset-Modelle sollten markiert werden](#)
- [\[IoTSiteWise.2\] AWS SiteWise IoT-Dashboards sollten markiert werden](#)
- [\[IoTSiteWise.3\] AWS SiteWise IoT-Gateways sollten markiert werden](#)
- [\[IoTSiteWise.4\] AWS SiteWise IoT-Portale sollten markiert werden](#)
- [\[IoTSiteWise.5\] AWS SiteWise IoT-Projekte sollten markiert werden](#)
- [\[IoT Twin Maker.1\] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden](#)
- [\[IoT Twin Maker.2\] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden](#)

- [\[Io TTwin Maker.3\] AWS TwinMaker IoT-Szenen sollten markiert werden](#)
- [\[Io TTwin Maker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[Io TWireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[Io TWireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)
- [\[Io TWireless .3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)
- [\[RDS.14\] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein](#)
- [\[RDS.31\] RDS-DB-Sicherheitsgruppen sollten markiert werden](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WorkSpaces.1\] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden](#)
- [\[WorkSpaces.2\] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden](#)

Europa (Zürich)

Die folgenden Steuerelemente werden in der Region Europa (Zürich) nicht unterstützt.

- [\[APIGateway.8\] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben](#)
- [\[APIGateway.9\] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein](#)
- [\[Amplify.1\] Amplify-Apps sollten markiert werden](#)
- [\[Amplify.2\] Amplify-Zweige sollten markiert werden](#)
- [\[AppConfig.1\] AWS AppConfig Anwendungen sollten markiert werden](#)
- [\[AppConfig.2\] AWS AppConfig Konfigurationsprofile sollten mit Tags versehen werden](#)

- [\[AppConfig.3\] AWS AppConfig Umgebungen sollten markiert werden](#)
- [\[AppFlow.1\] AppFlow Amazon-Datenflüsse sollten mit Tags versehen werden](#)
- [\[AppRunner.1\] App Runner-Dienste sollten markiert sein](#)
- [\[AppRunner.2\] App Runner VPC-Konnektoren sollten markiert sein](#)
- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [\[Backup.1\] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein](#)
- [\[Backup.4\] AWS Backup Berichtspläne sollten markiert werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[CloudTrail.6\] Sicherstellen, dass der S3-Bucket, in dem CloudTrail Protokolle gespeichert werden, nicht öffentlich zugänglich ist](#)
- [\[CloudTrail.7\] Sicherstellen, dass die S3-Bucket-Zugriffsprotokollierung für den CloudTrail S3-Bucket aktiviert ist](#)
- [\[CodeArtifact.1\] CodeArtifact Repositorien sollten mit Tags versehen werden](#)

- [\[CodeGuruProfiler.1\] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden](#)
- [\[CodeGuruReviewer.1\] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden](#)
- [\[Cognito.1\] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein](#)
- [\[Cognito.2\] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen](#)
- [\[Connect.1\] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden](#)
- [\[Connect.2\] Für Amazon Connect Connect-Instances sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[Detective.1\] Verhaltensdiagramme von Detektiven sollten markiert werden](#)
- [\[DMS.2\] DMS-Zertifikate sollten gekennzeichnet sein](#)
- [\[DMS.3\] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden](#)
- [\[DMS.4\] DMS-Replikationsinstanzen sollten markiert werden](#)
- [\[DMS.5\] Subnetzgruppen für die DMS-Replikation sollten markiert werden](#)
- [\[DMS.6\] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein](#)
- [\[DMS.7\] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.8\] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.9\] DMS-Endpunkte sollten SSL verwenden](#)
- [\[DMS.10\] Bei DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein](#)
- [\[DMS.11\] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein](#)
- [\[DMS.12\] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein](#)
- [\[DocumentDB.1\] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DocumentDB.2\] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen](#)
- [\[DocumentDB.3\] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein](#)
- [\[DocumentDB.4\] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch](#)

- [\[DocumentDB.5\] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[DocumentDB.6\] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[DynamoDB.3\] DynamoDB Accelerator \(DAX\) -Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DynamoDB.4\] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein](#)
- [\[DynamoDB.7\] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[EC2.4\] Gestoppte EC2 Instances sollten nach einem bestimmten Zeitraum entfernt werden](#)
- [\[EC2.8\] EC2 Instances sollten Instance Metadata Service Version 2 \(\) verwenden IMDSv2](#)
- [\[EC2.14\] Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 oder: :/0 auf Port 3389 zulassen](#)
- [\[EC2.22\] Ungenutzte EC2 Amazon-Sicherheitsgruppen sollten entfernt werden](#)
- [\[EC2.24\] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden](#)
- [\[EC2.25\] EC2 Amazon-Startvorlagen sollten Netzwerkschnittstellen nicht öffentlich IPs zuweisen](#)
- [\[EC2.28\] EBS-Volumes sollten durch einen Backup-Plan abgedeckt sein](#)
- [\[EC2.58\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert sein](#)
- [\[EC2.60\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden](#)
- [\[EC2.170\] EC2 Startvorlagen sollten Instance Metadata Service Version 2 \(\) verwenden IMDSv2](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[EC2.175\] EC2 Startvorlagen sollten mit Tags versehen sein](#)
- [\[EC2.180\] Bei EC2 Netzwerkschnittstellen sollte die source/destination Überprüfung aktiviert sein](#)
- [\[ECR.4\] Öffentliche ECR-Repositoryen sollten markiert werden](#)
- [\[EFS.1\] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS](#)
- [\[EFS.2\] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein](#)
- [\[ELB.2\] Classic Load Balancer mit SSL/HTTPS Listnern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager](#)
- [\[ELB.14\] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden](#)
- [\[ELB.17\] Anwendungs- und Netzwerk-Load-Balancer mit Listnern sollten die empfohlenen Sicherheitsrichtlinien verwenden](#)

- [\[ELB.18\] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln](#)
- [Bei \[ElastiCache.1\] ElastiCache \(Redis OSS\) -Clustern sollten automatische Backups aktiviert sein](#)
- [\[ElastiCache.6\] Für Replikationsgruppen ElastiCache \(Redis OSS\) früherer Versionen sollte Redis OSS AUTH aktiviert sein](#)
- [\[ElastiCache.7\] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden](#)
- [\[ElasticBeanstalk.1\] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben](#)
- [\[ElasticBeanstalk.2\] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk sollte Logs streamen nach CloudWatch](#)
- [\[EMR.1\] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben](#)
- [\[ES.4\] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein](#)
- [\[EventBridge.4\] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[Glue.4\] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue](#)
- [\[GuardDuty.2\] GuardDuty Filter sollten mit Tags versehen sein](#)
- [\[GuardDuty.3\] GuardDuty IPSets sollte markiert werden](#)
- [\[IAM.1\] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen](#)
- [\[IAM.2\] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein](#)
- [\[IAM.3\] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden](#)
- [\[IAM.4\] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren](#)
- [\[IAM.5\] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen](#)
- [\[IAM.8\] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden](#)
- [\[IAM.18\] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS -Support](#)

- [\[IAM.19\] MFA sollte für alle IAM-Benutzer aktiviert sein](#)
- [\[IAM.21\] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen](#)
- [\[IAM.22\] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden](#)
- [\[IAM.24\] IAM-Rollen sollten mit Tags versehen werden](#)
- [\[IAM.25\] IAM-Benutzer sollten markiert werden](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[IAM.27\] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloud ShellFullAccess](#)
- [\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)
- [\[IoT.1\] AWS IoT Device Defender Sicherheitsprofile sollten markiert werden](#)
- [\[IoT.2\] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden](#)
- [\[IoT.3\] AWS IoT Core -Dimensionen sollten markiert werden](#)
- [\[IoT.4\] AWS IoT Core Autorisierer sollten markiert werden](#)
- [\[IoT.5\] AWS IoT Core Rollenalias sollten markiert werden](#)
- [\[IoT.6\] AWS IoT Core Richtlinien sollten markiert werden](#)
- [\[IoTEvents .1\] AWS IoT-Events-Eingaben sollten markiert werden](#)
- [\[IoTEvents .2\] AWS IoT-Ereignisdetektormodelle sollten markiert werden](#)
- [\[IoTEvents .3\] Alarmmodelle für AWS IoT Events sollten markiert werden](#)
- [\[IoTSiteWise.1\] AWS SiteWise IoT-Asset-Modelle sollten markiert werden](#)
- [\[IoTSiteWise.2\] AWS SiteWise IoT-Dashboards sollten markiert werden](#)
- [\[IoTSiteWise.3\] AWS SiteWise IoT-Gateways sollten markiert werden](#)
- [\[IoTSiteWise.4\] AWS SiteWise IoT-Portale sollten markiert werden](#)
- [\[IoTSiteWise.5\] AWS SiteWise IoT-Projekte sollten markiert werden](#)
- [\[IoT Twin Maker.1\] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden](#)
- [\[IoT Twin Maker.2\] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden](#)
- [\[IoT Twin Maker.3\] AWS TwinMaker IoT-Szenen sollten markiert werden](#)
- [\[IoT Twin Maker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[IoT Wireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[IoT Wireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)

- [\[IoTWireless.3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)
- [\[Keyspaces.1\] Amazon Keyspaces Keyspaces sollten mit Tags versehen sein](#)
- [\[KMS.1\] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)
- [\[KMS.2\] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)
- [\[Lambda.7\] Bei Lambda-Funktionen sollte aktives Tracing aktiviert sein AWS X-Ray](#)
- [\[Macie.1\] Amazon Macie sollte aktiviert sein](#)
- [\[Macie.2\] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein](#)
- [\[MQ.2\] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch](#)
- [\[MQ.3\] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein](#)
- [\[MQ.4\] Amazon MQ-Broker sollten markiert werden](#)
- [\[MQ.5\] ActiveMQ-Broker sollten den Aktiv-/Standby-Bereitstellungsmodus verwenden](#)
- [\[MQ.6\] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden](#)
- [\[MSK.3\] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden](#)
- [\[MSK.4\] Bei MSK-Clustern sollte der öffentliche Zugriff deaktiviert sein](#)
- [\[MSK.5\] Bei MSK-Konnektoren sollte die Protokollierung aktiviert sein](#)
- [\[MSK.6\] MSK-Cluster sollten den nicht authentifizierten Zugriff deaktivieren](#)
- [\[Neptune.1\] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.2\] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)
- [\[Neptune.3\] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein](#)
- [\[Neptune.4\] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[Neptune.5\] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein](#)
- [\[Neptune.6\] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.7\] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein](#)
- [\[Neptune.8\] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren](#)
- [\[Neptune.9\] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden](#)

- [Bei \[Opensearch.1\] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein](#)
- [\[Opensearch.2\] OpenSearch -Domains sollten nicht öffentlich zugänglich sein](#)
- [\[Opensearch.3\] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden](#)
- [Die Protokollierung von \[Opensearch.4\] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein](#)
- [Für \[Opensearch.5\] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein](#)
- [\[Opensearch.6\] OpenSearch Domains sollten mindestens drei Datenknoten haben](#)
- [Für \[Opensearch.7\] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein](#)
- [\[Opensearch.8\] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden](#)
- [\[Opensearch.9\] OpenSearch -Domains sollten mit Tags versehen werden](#)
- [Auf \[Opensearch.10\] OpenSearch -Domains sollte das neueste Softwareupdate installiert sein](#)
- [\[Opensearch.11\] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben](#)
- [\[RDS.1\] Der RDS-Snapshot sollte privat sein](#)
- [\[RDS.14\] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein](#)
- [\[RDS.26\] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden](#)
- [\[RDS.31\] RDS-DB-Sicherheitsgruppen sollten markiert werden](#)
- [\[RDS.35\] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein](#)
- [\[Redshift.18\] Für Redshift-Cluster sollten Multi-AZ-Bereitstellungen aktiviert sein](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)
- [\[SageMaker.1\] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben](#)
- [\[SageMaker.2\] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden](#)
- [\[SageMaker.3\] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben](#)
- [\[SageMaker.5\] SageMaker Modelle sollten eingehenden Datenverkehr blockieren](#)

- [\[SageMaker.6\] SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden](#)
- [\[SageMaker.7\] SageMaker Bilder sollten mit Tags versehen werden](#)
- [\[SES.1\] SES-Kontaktlisten sollten mit Tags versehen werden](#)
- [\[SES.2\] SES-Konfigurationssätze sollten mit Tags versehen werden](#)
- [\[SQS.1\] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt werden](#)
- [\[SQS.2\] SQS-Warteschlangen sollten markiert werden](#)
- [\[SQS.3\] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen](#)
- [\[SSM.3\] Von Systems Manager verwaltete EC2 Amazon-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben](#)
- [\[SSM.6\] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[SSM.7\] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein](#)
- [\[Transfer.3\] Bei Connectoren der Transfer-Familie sollte die Protokollierung aktiviert sein](#)
- [\[Transfer.4\] Transfer Family Familienverträge sollten gekennzeichnet werden](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.3\] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WAF.10\] AWS WAF web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WAF.11\] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WorkSpaces.1\] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden](#)
- [\[WorkSpaces.2\] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden](#)

Israel (Tel Aviv)

Die folgenden Kontrollen werden in der Region Israel (Tel Aviv) nicht unterstützt.

- [\[APIGateway.8\] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben](#)
- [\[APIGateway.9\] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein](#)
- [\[Amplify.1\] Amplify-Apps sollten markiert werden](#)

- [\[Amplify.2\] Amplify-Zweige sollten markiert werden](#)
- [\[AppFlow.1\] AppFlow Amazon-Datenflüsse sollten mit Tags versehen werden](#)
- [\[AppRunner.1\] App Runner-Dienste sollten markiert sein](#)
- [\[AppRunner.2\] App Runner VPC-Konnektoren sollten markiert sein](#)
- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.2\] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben](#)
- [\[AppSync.5\] AWS AppSync GraphQL APIs sollte nicht mit API-Schlüsseln authentifiziert werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [\[Backup.1\] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein](#)
- [\[Backup.4\] AWS Backup Berichtspläne sollten markiert werden](#)
- [\[Batch.1\] Warteschlangen für Batch-Jobs sollten markiert werden](#)
- [\[Batch.3\] Batch-Computing-Umgebungen sollten markiert werden](#)
- [\[Batch.4\] Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)

- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[CodeArtifact.1\] CodeArtifact Repositorien sollten mit Tags versehen werden](#)
- [\[CodeGuruProfiler.1\] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden](#)
- [\[CodeGuruReviewer.1\] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden](#)
- [\[Cognito.2\] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen](#)
- [\[Connect.1\] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden](#)
- [\[Connect.2\] Für Amazon Connect Connect-Instances sollte die Protokollierung aktiviert sein](#)
[CloudWatch](#)
- [\[DMS.2\] DMS-Zertifikate sollten gekennzeichnet sein](#)
- [\[DMS.3\] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden](#)
- [\[DMS.4\] DMS-Replikationsinstanzen sollten markiert werden](#)
- [\[DMS.5\] Subnetzgruppen für die DMS-Replikation sollten markiert werden](#)
- [\[DMS.6\] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein](#)
- [\[DMS.7\] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.8\] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.9\] DMS-Endpunkte sollten SSL verwenden](#)
- [\[DMS.10\] Bei DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein](#)
- [\[DMS.11\] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein](#)
- [\[DMS.12\] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein](#)
- [\[DocumentDB.1\] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DocumentDB.2\] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen](#)
- [\[DocumentDB.3\] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein](#)
- [\[DocumentDB.4\] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen](#)
[CloudWatch](#)

- [\[DocumentDB.5\] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[DocumentDB.6\] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[DynamoDB.3\] DynamoDB Accelerator \(DAX\) -Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DynamoDB.4\] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein](#)
- [\[DynamoDB.7\] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[EC2.4\] Gestoppte EC2 Instances sollten nach einem bestimmten Zeitraum entfernt werden](#)
- [\[EC2.14\] Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 oder: :/0 auf Port 3389 zulassen](#)
- [\[EC2.20\] Beide VPN-Tunnel für eine AWS Site-to-Site VPN-Verbindung sollten aktiv sein](#)
- [\[EC2.22\] Ungenutzte EC2 Amazon-Sicherheitsgruppen sollten entfernt werden](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways sollte VPC-Anhangsanfragen nicht automatisch akzeptieren](#)
- [\[EC2.24\] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden](#)
- [\[EC2.25\] EC2 Amazon-Startvorlagen sollten Netzwerkschnittstellen nicht öffentlich IPs zuweisen](#)
- [\[EC2.28\] EBS-Volumes sollten durch einen Backup-Plan abgedeckt sein](#)
- [\[EC2.33\] EC2 Transit-Gateway-Anhänge sollten mit Tags versehen werden](#)
- [\[EC2.34\] Die Routentabellen für EC2 Transit-Gateways sollten mit Tags versehen werden](#)
- [\[EC2.40\] EC2 NAT-Gateways sollten markiert werden](#)
- [\[EC2.48\] Amazon VPC-Flow-Logs sollten mit Tags versehen werden](#)
- [\[EC2.51\] EC2 Client-VPN-Endpunkte sollten die Client-Verbindungsprotokollierung aktiviert haben](#)
- [\[EC2.55\] VPCs sollte mit einem Schnittstellenendpunkt für die ECR-API konfiguriert werden](#)
- [\[EC2.56\] VPCs sollte mit einem Schnittstellenendpunkt für Docker Registry konfiguriert werden](#)
- [\[EC2.57\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager konfiguriert werden](#)
- [\[EC2.58\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert sein](#)
- [\[EC2.60\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden](#)
- [\[EC2.170\] EC2 Startvorlagen sollten Instance Metadata Service Version 2 \(\) verwenden IMDSv2](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[EC2.175\] EC2 Startvorlagen sollten mit Tags versehen sein](#)

- [\[EC2.177\] EC2 Traffic Mirror-Sitzungen sollten mit Tags versehen werden](#)
- [\[EC2.179\] EC2 Traffic-Spiegel-Ziele sollten markiert werden](#)
- [\[EC2.180\] Bei EC2 Netzwerkschnittstellen sollte die source/destination Überprüfung aktiviert sein](#)
- [\[ECR.2\] Bei privaten ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein](#)
- [\[ECR.3\] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein](#)
- [\[ECR.4\] Öffentliche ECR-Repositorien sollten markiert werden](#)
- [\[ECR.5\] ECR-Repositorys sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys](#)
- [\[ECS.16\] ECS-Aufgabensätze sollten öffentliche IP-Adressen nicht automatisch zuweisen](#)
- [\[EFS.1\] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS](#)
- [\[EFS.2\] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein](#)
- [\[EFS.3\] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen](#)
- [\[EFS.4\] EFS-Zugangspunkte sollten eine Benutzeridentität erzwingen](#)
- [\[EFS.8\] EFS-Dateisysteme sollten im Ruhezustand verschlüsselt werden](#)
- [\[EKS.2\] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden](#)
- [\[EKS.6\] EKS-Cluster sollten markiert werden](#)
- [\[EKS.7\] Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden](#)
- [\[EKS.8\] Bei EKS-Clustern sollte die Auditprotokollierung aktiviert sein](#)
- [\[ELB.2\] Classic Load Balancer mit SSL/HTTPS Listnern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager](#)
- [\[ELB.14\] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden](#)
- [\[ELB.17\] Anwendungs- und Netzwerk-Load-Balancer mit Listnern sollten die empfohlenen Sicherheitsrichtlinien verwenden](#)
- [\[ELB.18\] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln](#)
- [Bei \[ElastiCache.1\] ElastiCache \(Redis OSS\) -Clustern sollten automatische Backups aktiviert sein](#)
- [\[ElastiCache.2\] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein](#)
- [\[ElastiCache.3\] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein](#)
- [\[ElastiCache.4\] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden](#)

- [\[ElastiCache.5\] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden](#)
- [\[ElastiCache.6\] Für Replikationsgruppen ElastiCache \(Redis OSS\) früherer Versionen sollte Redis OSS AUTH aktiviert sein](#)
- [\[ElastiCache.7\] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden](#)
- [\[ElasticBeanstalk.1\] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben](#)
- [\[ElasticBeanstalk.2\] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk sollte Logs streamen nach CloudWatch](#)
- [\[EMR.1\] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben](#)
- [\[EMR.3\] Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden](#)
- [\[ES.4\] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein](#)
- [\[EventBridge.4\] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[Glue.4\] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue](#)
- [\[GuardDuty.2\] GuardDuty Filter sollten mit Tags versehen sein](#)
- [\[GuardDuty.3\] GuardDuty IPSets sollte markiert werden](#)
- [\[IAM.1\] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen](#)
- [\[IAM.2\] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein](#)
- [\[IAM.3\] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden](#)
- [\[IAM.4\] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren](#)
- [\[IAM.5\] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen](#)
- [\[IAM.6\] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.](#)
- [\[IAM.7\] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein](#)
- [\[IAM.8\] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden](#)
- [\[IAM.9\] MFA sollte für den Root-Benutzer aktiviert sein](#)

- [\[IAM.10\] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein](#)
- [\[IAM.11\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert](#)
- [\[IAM.12\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert](#)
- [\[IAM.13\] Stellen Sie sicher, dass für die IAM-Passwortrichtlinie mindestens ein Symbol erforderlich ist](#)
- [\[IAM.14\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert](#)
- [\[IAM.15\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert](#)
- [\[IAM.16\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert](#)
- [\[IAM.17\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft](#)
- [\[IAM.18\] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS -Support](#)
- [\[IAM.19\] MFA sollte für alle IAM-Benutzer aktiviert sein](#)
- [\[IAM.21\] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen](#)
- [\[IAM.22\] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden](#)
- [\[IAM.24\] IAM-Rollen sollten mit Tags versehen werden](#)
- [\[IAM.25\] IAM-Benutzer sollten markiert werden](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[IAM.27\] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWS Cloud Shell Full Access](#)
- [\[IAM.28\] Der externe Zugriffsanalysator für IAM Access Analyzer sollte aktiviert sein](#)
- [\[Inspector.1\] Das EC2 Scannen mit Amazon Inspector sollte aktiviert sein](#)
- [\[Inspector.2\] Das Amazon Inspector ECR-Scannen sollte aktiviert sein](#)
- [\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)
- [\[Inspector.4\] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein](#)
- [\[IoT.1\] AWS IoT Device Defender Sicherheitsprofile sollten markiert werden](#)
- [\[IoT.2\] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden](#)

- [\[IoT.3\] AWS IoT Core -Dimensionen sollten markiert werden](#)
- [\[IoT.4\] AWS IoT Core Autorisierer sollten markiert werden](#)
- [\[IoT.5\] AWS IoT Core Rollenalias sollten markiert werden](#)
- [\[IoT.6\] AWS IoT Core Richtlinien sollten markiert werden](#)
- [\[IoTEvents .1\] AWS IoT-Events-Eingaben sollten markiert werden](#)
- [\[IoTEvents .2\] AWS IoT-Ereignisdetektormodelle sollten markiert werden](#)
- [\[IoTEvents .3\] Alarmmodelle für AWS IoT Events sollten markiert werden](#)
- [\[IoTSiteWise.1\] AWS SiteWise IoT-Asset-Modelle sollten markiert werden](#)
- [\[IoTSiteWise.2\] AWS SiteWise IoT-Dashboards sollten markiert werden](#)
- [\[IoTSiteWise.3\] AWS SiteWise IoT-Gateways sollten markiert werden](#)
- [\[IoTSiteWise.4\] AWS SiteWise IoT-Portale sollten markiert werden](#)
- [\[IoTSiteWise.5\] AWS SiteWise IoT-Projekte sollten markiert werden](#)
- [\[IOTwinMaker.1\] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden](#)
- [\[IOTwinMaker.2\] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden](#)
- [\[IOTwinMaker.3\] AWS TwinMaker IoT-Szenen sollten markiert werden](#)
- [\[IOTwinMaker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[IOWireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[IOWireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)
- [\[IOWireless .3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)
- [\[Keyspaces.1\] Amazon Keyspaces Keyspaces sollten mit Tags versehen sein](#)
- [\[Kinesis.1\] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden](#)
- [\[Kinesis.2\] Kinesis-Streams sollten markiert werden](#)
- [\[Kinesis.3\] Kinesis-Streams sollten über eine angemessene Aufbewahrungsfrist für Daten verfügen](#)
- [\[KMS.1\] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)
- [\[KMS.2\] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)

- [\[Lambda.5\] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren](#)
- [\[Lambda.7\] Bei Lambda-Funktionen sollte aktives Tracing aktiviert sein AWS X-Ray](#)
- [\[Macie.1\] Amazon Macie sollte aktiviert sein](#)
- [\[MQ.2\] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch](#)
- [\[MQ.3\] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein](#)
- [\[MQ.4\] Amazon MQ-Broker sollten markiert werden](#)
- [\[MQ.5\] ActiveMQ-Broker sollten den Aktiv-/Standby-Bereitstellungsmodus verwenden](#)
- [\[MQ.6\] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden](#)
- [\[MSK.1\] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden](#)
- [\[MSK.2\] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein](#)
- [\[MSK.3\] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden](#)
- [\[MSK.4\] Bei MSK-Clustern sollte der öffentliche Zugriff deaktiviert sein](#)
- [\[MSK.5\] Bei MSK-Konnektoren sollte die Protokollierung aktiviert sein](#)
- [\[MSK.6\] MSK-Cluster sollten den nicht authentifizierten Zugriff deaktivieren](#)
- [\[Neptune.3\] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein](#)
- [\[Neptune.6\] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden](#)
- [\[NetworkFirewall.10\] Bei Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein](#)
- [Bei \[Opensearch.1\] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein](#)
- [\[Opensearch.2\] OpenSearch -Domains sollten nicht öffentlich zugänglich sein](#)
- [\[Opensearch.3\] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden](#)
- [Die Protokollierung von \[Opensearch.4\] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein](#)
- [Für \[Opensearch.5\] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein](#)
- [\[Opensearch.6\] OpenSearch Domains sollten mindestens drei Datenknoten haben](#)
- [Für \[Opensearch.7\] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein](#)
- [\[Opensearch.8\] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden](#)
- [\[Opensearch.9\] OpenSearch -Domains sollten mit Tags versehen werden](#)

- [\[Opensearch.10\] OpenSearch -Domains sollte das neueste Softwareupdate installiert sein](#)
- [\[Opensearch.11\] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben](#)
- [\[RDS.1\] Der RDS-Snapshot sollte privat sein](#)
- [\[RDS.4\] RDS-Cluster-Snapshots und Datenbank-Snapshots sollten im Ruhezustand verschlüsselt werden](#)
- [\[RDS.14\] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein](#)
- [\[RDS.15\] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden](#)
- [\[RDS.26\] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden](#)
- [\[RDS.29\] RDS-DB-Cluster-Snapshots sollten markiert werden](#)
- [\[RDS.31\] RDS-DB-Sicherheitsgruppen sollten markiert werden](#)
- [\[RDS.35\] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein](#)
- [\[RDS.37\] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[Redshift.3\] Bei Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein](#)
- [\[Redshift.8\] Amazon Redshift Redshift-Cluster sollten nicht den standardmäßigen Admin-Benutzernamen verwenden](#)
- [\[Redshift.9\] Redshift-Cluster sollten nicht den Standard-Datenbanknamen verwenden](#)
- [\[Redshift.18\] Für Redshift-Cluster sollten Multi-AZ-Bereitstellungen aktiviert sein](#)
- [\[RedshiftServerless.1\] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden](#)
- [\[RedshiftServerless.2\] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)
- [\[SageMaker.1\] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben](#)
- [\[SageMaker.2\] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden](#)
- [\[SageMaker.3\] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben](#)

- [\[SageMaker.5\] SageMaker Modelle sollten eingehenden Datenverkehr blockieren](#)
- [\[ServiceCatalog.1\] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden](#)
- [\[SQS.1\] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt werden](#)
- [\[SQS.2\] SQS-Warteschlangen sollten markiert werden](#)
- [\[SQS.3\] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen](#)
- [\[SSM.3\] Von Systems Manager verwaltete EC2 Amazon-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben](#)
- [\[SSM.4\] SSM-Dokumente sollten nicht öffentlich sein](#)
- [\[SSM.6\] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[SSM.7\] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein](#)
- [\[StepFunctions.1\] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben](#)
- [\[Transfer.3\] Bei Connectoren der Transfer-Familie sollte die Protokollierung aktiviert sein](#)
- [\[Transfer.4\] Transfer Family Familienverträge sollten gekennzeichnet werden](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.3\] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WAF.11\] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WorkSpaces.1\] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden](#)
- [\[WorkSpaces.2\] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden](#)

Mexiko (Zentral)

Die folgenden Steuerelemente werden in der Region Mexiko (Zentral) nicht unterstützt.

- [\[ACM.1\] Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden](#)

- [\[ACM.2\] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden](#)
- [\[ACM.3\] ACM-Zertifikate sollten mit einem Tag versehen werden](#)
- [\[Account.1\] Sicherheitskontaktinformationen sollten bereitgestellt werden für AWS-Konto](#)
- [\[Account.2\] AWS-Konten sollte Teil einer Organisation sein AWS Organizations](#)
- [\[APIGateway.1\] API Gateway REST und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein](#)
- [\[APIGateway.2\] API Gateway REST API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden](#)
- [\[APIGateway.3\] Bei den REST-API-Stufen von API Gateway sollte die AWS X-Ray Ablaufverfolgung aktiviert sein](#)
- [\[APIGateway.4\] API Gateway sollte mit einer WAF-Web-ACL verknüpft sein](#)
- [\[APIGateway.5\] API Gateway REST API-Cache-Daten sollten im Ruhezustand verschlüsselt werden](#)
- [\[APIGateway.8\] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben](#)
- [\[APIGateway.9\] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein](#)
- [\[Amplify.1\] Amplify-Apps sollten markiert werden](#)
- [\[Amplify.2\] Amplify-Zweige sollten markiert werden](#)
- [\[AppConfig.1\] AWS AppConfig Anwendungen sollten markiert werden](#)
- [\[AppConfig.2\] AWS AppConfig Konfigurationsprofile sollten mit Tags versehen werden](#)
- [\[AppConfig.3\] AWS AppConfig Umgebungen sollten markiert werden](#)
- [\[AppConfig.4\] AWS AppConfig Erweiterungszuordnungen sollten markiert werden](#)
- [\[AppFlow.1\] AppFlow Amazon-Datenflüsse sollten mit Tags versehen werden](#)
- [\[AppRunner.1\] App Runner-Dienste sollten markiert sein](#)
- [\[AppRunner.2\] App Runner VPC-Konnektoren sollten markiert sein](#)
- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.2\] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben](#)
- [\[AppSync.4\] AWS AppSync GraphQL APIs sollte markiert sein](#)
- [\[AppSync.5\] AWS AppSync GraphQL APIs sollte nicht mit API-Schlüsseln authentifiziert werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [\[Athena.2\] Athena-Datenkataloge sollten mit Tags versehen werden](#)

- [\[Athena.3\] Athena-Arbeitsgruppen sollten markiert werden](#)
- [\[Athena.4\] Bei Athena-Arbeitsgruppen sollte die Protokollierung aktiviert sein](#)
- [\[AutoScaling.2\] Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken](#)
- [\[AutoScaling.3\] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2 Instances so konfigurieren, dass sie Instance Metadata Service Version 2 \(IMDSv2\) benötigen](#)
- [\[AutoScaling.6\] Auto Scaling Scaling-Gruppen sollten mehrere Instance-Typen in mehreren Availability Zones verwenden](#)
- [\[AutoScaling.9\] Amazon EC2 Auto Scaling Scaling-Gruppen sollten EC2 Amazon-Startvorlagen verwenden](#)
- [\[AutoScaling.10\] EC2 Auto Scaling Scaling-Gruppen sollten markiert werden](#)
- [\[Backup.1\] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein](#)
- [\[Backup.2\] AWS Backup Wiederherstellungspunkte sollten markiert werden](#)
- [\[Backup.3\] AWS Backup Tresore sollten markiert sein](#)
- [\[Backup.4\] AWS Backup Berichtspläne sollten markiert werden](#)
- [\[Backup.5\] AWS Backup Backup-Pläne sollten markiert werden](#)
- [\[Batch.1\] Warteschlangen für Batch-Jobs sollten markiert werden](#)
- [\[Batch.2\] Richtlinien für die Batch-Planung sollten gekennzeichnet sein](#)
- [\[Batch.3\] Batch-Computing-Umgebungen sollten markiert werden](#)
- [\[Batch.4\] Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden](#)
- [\[CloudFormation.2\] CloudFormation Stapel sollten markiert werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)

- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[CloudTrail.6\] Sicherstellen, dass der S3-Bucket, in dem CloudTrail Protokolle gespeichert werden, nicht öffentlich zugänglich ist](#)
- [\[CloudTrail.7\] Sicherstellen, dass die S3-Bucket-Zugriffsprotokollierung für den CloudTrail S3-Bucket aktiviert ist](#)
- [\[CloudTrail.9\] CloudTrail Pfade sollten markiert werden](#)
- [\[CloudTrail.10\] Event-Datenspeicher in CloudTrail Lake sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys](#)
- [\[CloudWatch.17\] CloudWatch Alarmaktionen sollten aktiviert sein](#)
- [\[CodeArtifact.1\] CodeArtifact Repositorien sollten mit Tags versehen werden](#)
- [\[CodeBuild.1\] Das CodeBuild Bitbucket-Quell-Repository URLs sollte keine vertraulichen Anmeldeinformationen enthalten](#)
- [\[CodeBuild.2\] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten](#)
- [\[CodeBuild.3\] CodeBuild S3-Protokolle sollten verschlüsselt sein](#)
- [\[CodeBuild.4\] CodeBuild Projektumgebungen sollten eine AWS Config Protokollierungsdauer haben](#)
- [\[CodeBuild.7\] Exporte von CodeBuild Berichtsgruppen sollten im Ruhezustand verschlüsselt werden](#)
- [\[CodeGuruProfiler.1\] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden](#)
- [\[CodeGuruReviewer.1\] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden](#)
- [\[Cognito.1\] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein](#)

- [\[Cognito.2\] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen](#)
- [\[Connect.1\] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden](#)
- [\[Connect.2\] Für Amazon Connect Connect-Instances sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[DataFirehose.1\] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden](#)
- [\[DataSync.1\] Für DataSync Aufgaben sollte die Protokollierung aktiviert sein](#)
- [\[DataSync.2\] DataSync Aufgaben sollten mit Tags versehen werden](#)
- [\[Detective.1\] Verhaltensdiagramme von Detektiven sollten markiert werden](#)
- [\[DMS.1\] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein](#)
- [\[DMS.2\] DMS-Zertifikate sollten gekennzeichnet sein](#)
- [\[DMS.3\] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden](#)
- [\[DMS.4\] DMS-Replikationsinstanzen sollten markiert werden](#)
- [\[DMS.5\] Subnetzgruppen für die DMS-Replikation sollten markiert werden](#)
- [\[DMS.6\] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein](#)
- [\[DMS.7\] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.8\] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.9\] DMS-Endpunkte sollten SSL verwenden](#)
- [\[DMS.10\] Bei DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein](#)
- [\[DMS.11\] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein](#)
- [\[DMS.12\] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein](#)
- [\[DocumentDB.1\] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DocumentDB.2\] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen](#)
- [\[DocumentDB.3\] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein](#)
- [\[DocumentDB.4\] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch](#)

- [\[DocumentDB.5\] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[DocumentDB.6\] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[DynamoDB.3\] DynamoDB Accelerator \(DAX\) -Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DynamoDB.4\] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein](#)
- [\[DynamoDB.5\] DynamoDB-Tabellen sollten mit Tags versehen werden](#)
- [\[DynamoDB.6\] Bei DynamoDB-Tabellen sollte der Löschschutz aktiviert sein](#)
- [\[DynamoDB.7\] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[EC2.4\] Gestoppte EC2 Instances sollten nach einem bestimmten Zeitraum entfernt werden](#)
- [\[EC2.21\] Das Netzwerk ACLs sollte keinen Zugang von 0.0.0.0/0 zu Port 22 oder Port 3389 zulassen](#)
- [\[EC2.22\] Ungenutzte EC2 Amazon-Sicherheitsgruppen sollten entfernt werden](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways sollte VPC-Anhangsanfragen nicht automatisch akzeptieren](#)
- [\[EC2.24\] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden](#)
- [\[EC2.25\] EC2 Amazon-Startvorlagen sollten Netzwerkschnittstellen nicht öffentlich IPs zuweisen](#)
- [\[EC2.28\] EBS-Volumes sollten durch einen Backup-Plan abgedeckt sein](#)
- [\[EC2.33\] EC2 Transit-Gateway-Anhänge sollten mit Tags versehen werden](#)
- [\[EC2.34\] Die Routentabellen für EC2 Transit-Gateways sollten mit Tags versehen werden](#)
- [\[EC2.35\] EC2 Netzwerkschnittstellen sollten markiert werden](#)
- [\[EC2.36\] EC2 Kunden-Gateways sollten mit Tags versehen werden](#)
- [\[EC2.37\] EC2 Elastische IP-Adressen sollten mit Tags versehen werden](#)
- [\[EC2.38\] EC2 Instances sollten markiert werden](#)
- [\[EC2.39\] EC2 Internet-Gateways sollten markiert werden](#)
- [\[EC2.40\] EC2 NAT-Gateways sollten markiert werden](#)
- [\[EC2.41\] Das EC2 Netzwerk ACLs sollte markiert sein](#)
- [\[EC2.42\] EC2 Routing-Tabellen sollten mit Tags versehen werden](#)
- [\[EC2.43\] EC2 Sicherheitsgruppen sollten markiert werden](#)
- [\[EC2.44\] EC2 Subnetze sollten markiert werden](#)
- [\[EC2.45\] EC2 Volumen sollten mit Tags versehen werden](#)
- [\[EC2.46\] Amazon VPCs sollte markiert werden](#)

- [\[EC2.47\] Amazon VPC Endpoint Services sollten markiert werden](#)
- [\[EC2.48\] Amazon VPC-Flow-Logs sollten mit Tags versehen werden](#)
- [\[EC2.49\] Amazon VPC-Peering-Verbindungen sollten markiert werden](#)
- [\[EC2.50\] EC2 VPN-Gateways sollten markiert werden](#)
- [\[EC2.51\] EC2 Client-VPN-Endpunkte sollten die Client-Verbindungsprotokollierung aktiviert haben](#)
- [\[EC2.52\] EC2 Transit-Gateways sollten markiert werden](#)
- [\[EC2.53\] EC2 Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 zu Remote-Serververwaltungsports zulassen](#)
- [\[EC2.54\] EC2 Sicherheitsgruppen sollten keinen Zugriff von: :/0 zu Remote-Serveradministrationsports zulassen](#)
- [\[EC2.55\] VPCs sollte mit einem Schnittstellenendpunkt für die ECR-API konfiguriert werden](#)
- [\[EC2.56\] VPCs sollte mit einem Schnittstellenendpunkt für Docker Registry konfiguriert werden](#)
- [\[EC2.57\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager konfiguriert werden](#)
- [\[EC2.58\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert sein](#)
- [\[EC2.60\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden](#)
- [\[EC2.170\] EC2 Startvorlagen sollten Instance Metadata Service Version 2 \(\) verwenden IMDSv2](#)
- [\[EC2.171\] Bei EC2 VPN-Verbindungen sollte die Protokollierung aktiviert sein](#)
- [\[EC2.172\] Die Einstellungen von EC2 VPC Block Public Access sollten den Internet-Gateway-Verkehr blockieren](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[EC2.174\] EC2 DHCP-Optionssätze sollten mit Tags versehen werden](#)
- [\[EC2.175\] EC2 Startvorlagen sollten mit Tags versehen sein](#)
- [\[EC2.176\] EC2 Präfixlisten sollten mit Tags versehen werden](#)
- [\[EC2.177\] EC2 Traffic Mirror-Sitzungen sollten mit Tags versehen werden](#)
- [\[EC2.178\] Filter für EC2 Verkehrsspiegel sollten mit Tags versehen werden](#)
- [\[EC2.179\] EC2 Traffic-Spiegel-Ziele sollten markiert werden](#)
- [\[EC2.180\] Bei EC2 Netzwerkschnittstellen sollte die source/destination Überprüfung aktiviert sein](#)
- [\[ECR.1\] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein](#)

- [\[ECR.2\] Bei privaten ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein](#)
- [\[ECR.3\] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein](#)
- [\[ECR.4\] Öffentliche ECR-Repositoryn sollten markiert werden](#)
- [\[ECR.5\] ECR-Repositorys sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys](#)
- [\[ECS.2\] ECS-Diensten sollten nicht automatisch öffentliche IP-Adressen zugewiesen werden](#)
- [\[ECS.3\] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen](#)
- [\[ECS.4\] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden](#)
- [\[ECS.5\] ECS-Container sollten auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sein](#)
- [\[ECS.8\] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden](#)
- [\[ECS.9\] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen](#)
- [\[ECS.10\] Die ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen](#)
- [\[ECS.12\] ECS-Cluster sollten Container Insights verwenden](#)
- [\[ECS.13\] ECS-Services sollten markiert werden](#)
- [\[ECS.14\] ECS-Cluster sollten markiert werden](#)
- [\[ECS.15\] ECS-Aufgabendefinitionen sollten mit Tags versehen werden](#)
- [\[ECS.16\] ECS-Aufgabensätze sollten öffentliche IP-Adressen nicht automatisch zuweisen](#)
- [\[ECS.17\] ECS-Aufgabendefinitionen sollten nicht den Host-Netzwerkmodus verwenden](#)
- [\[EFS.1\] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS](#)
- [\[EFS.2\] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein](#)
- [\[EFS.3\] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen](#)
- [\[EFS.4\] EFS-Zugangspunkte sollten eine Benutzeridentität erzwingen](#)
- [\[EFS.5\] EFS-Zugangspunkte sollten markiert werden](#)
- [\[EFS.6\] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden](#)
- [\[EFS.7\] Bei EFS-Dateisystemen sollten automatische Backups aktiviert sein](#)
- [\[EFS.8\] EFS-Dateisysteme sollten im Ruhezustand verschlüsselt werden](#)
- [\[EKS.2\] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden](#)
- [\[EKS.3\] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden](#)
- [\[EKS.6\] EKS-Cluster sollten markiert werden](#)

- [\[EKS.7\] Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden](#)
- [\[EKS.8\] Bei EKS-Clustern sollte die Auditprotokollierung aktiviert sein](#)
- [\[ELB.7\] Bei Classic Load Balancern sollte der Verbindungsabbau aktiviert sein](#)
- [\[ELB.10\] Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken](#)
- [\[ELB.12\] Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden](#)
- [\[ELB.13\] Anwendungs-, Netzwerk- und Gateway-Load Balancer sollten sich über mehrere Availability Zones erstrecken](#)
- [\[ELB.14\] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden](#)
- [\[ELB.17\] Anwendungs- und Netzwerk-Load-Balancer mit Listenern sollten die empfohlenen Sicherheitsrichtlinien verwenden](#)
- [\[ELB.18\] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln](#)
- [Bei \[ElastiCache.1\] ElastiCache \(Redis OSS\) -Clustern sollten automatische Backups aktiviert sein](#)
- [\[ElastiCache.2\] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein](#)
- [\[ElastiCache.3\] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein](#)
- [\[ElastiCache.4\] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden](#)
- [\[ElastiCache.5\] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden](#)
- [\[ElastiCache.6\] Für Replikationsgruppen ElastiCache \(Redis OSS\) früherer Versionen sollte Redis OSS AUTH aktiviert sein](#)
- [\[ElastiCache.7\] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden](#)
- [\[ElasticBeanstalk.1\] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben](#)
- [\[ElasticBeanstalk.2\] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk sollte Logs streamen nach CloudWatch](#)
- [\[EMR.1\] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben](#)
- [\[EMR.2\] Die Amazon EMR-Einstellung zum Blockieren des öffentlichen Zugriffs sollte aktiviert sein](#)
- [\[EMR.3\] Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden](#)
- [\[EMR.4\] Amazon EMR-Sicherheitskonfigurationen sollten bei der Übertragung verschlüsselt werden](#)

- [\[ES.3\] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden](#)
- [\[ES.4\] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein](#)
- [\[ES.5\] Für Elasticsearch-Domains sollte die Audit-Protokollierung aktiviert sein](#)
- [\[ES.6\] Elasticsearch-Domains sollten mindestens drei Datenknoten haben](#)
- [\[ES.7\] Elasticsearch-Domänen sollten mit mindestens drei dedizierten Master-Knoten konfiguriert werden](#)
- [\[ES.8\] Verbindungen zu Elasticsearch-Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden](#)
- [\[ES.9\] Elasticsearch-Domains sollten markiert werden](#)
- [\[EventBridge.2\] EventBridge Eventbusse sollten gekennzeichnet sein](#)
- [\[EventBridge.3\] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden](#)
- [\[EventBridge.4\] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[FSx.1\] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden](#)
- [\[FSx.2\] FSx für Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden](#)
- [\[FSx.3\] FSx für OpenZFS-Dateisysteme sollte für die Multi-AZ-Bereitstellung konfiguriert werden](#)
- [\[FSx.4\] FSx für NetApp ONTAP-Dateisysteme sollte für die Multi-AZ-Bereitstellung konfiguriert sein](#)
- [\[FSx.5\] FSx für Windows-Dateiserver sollten für die Multi-AZ-Bereitstellung konfiguriert sein](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[Glue.1\] AWS Glue Jobs sollten markiert werden](#)
- [\[Glue.3\] Transformationen für AWS Glue maschinelles Lernen sollten im Ruhezustand verschlüsselt werden](#)
- [\[Glue.4\] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue](#)
- [\[GuardDuty.1\] GuardDuty sollte aktiviert sein](#)
- [\[GuardDuty.2\] GuardDuty Filter sollten mit Tags versehen sein](#)

- [\[GuardDuty.3\] GuardDuty IPSets sollte markiert werden](#)
- [\[GuardDuty.4\] GuardDuty Detektoren sollten markiert werden](#)
- [\[GuardDuty.5\] GuardDuty EKS Audit Log Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.6\] GuardDuty Lambda Protection sollte aktiviert sein](#)
- [\[GuardDuty.7\] GuardDuty EKS Runtime Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.8\] Der GuardDuty Malware-Schutz für EC2 sollte aktiviert sein](#)
- [\[GuardDuty.9\] Der GuardDuty RDS-Schutz sollte aktiviert sein](#)
- [\[GuardDuty.10\] Der GuardDuty S3-Schutz sollte aktiviert sein](#)
- [\[GuardDuty.11\] GuardDuty Runtime Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.12\] GuardDuty ECS Runtime Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.13\] GuardDuty EC2 Runtime Monitoring sollte aktiviert sein](#)
- [\[IAM.1\] IAM-Richtlinien sollten keine vollen „*“-Administratorrechte zulassen](#)
- [\[IAM.2\] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein](#)
- [\[IAM.3\] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden](#)
- [\[IAM.4\] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren](#)
- [\[IAM.5\] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen](#)
- [\[IAM.6\] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.](#)
- [\[IAM.7\] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein](#)
- [\[IAM.8\] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden](#)
- [\[IAM.9\] MFA sollte für den Root-Benutzer aktiviert sein](#)
- [\[IAM.10\] Die Kennwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein](#)
- [\[IAM.11\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert](#)
- [\[IAM.12\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert](#)
- [\[IAM.13\] Stellen Sie sicher, dass für die IAM-Passwortrichtlinie mindestens ein Symbol erforderlich ist](#)
- [\[IAM.14\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert](#)
- [\[IAM.15\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert](#)

- [\[IAM.16\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert](#)
- [\[IAM.17\] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft](#)
- [\[IAM.18\] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS -Support](#)
- [\[IAM.19\] MFA sollte für alle IAM-Benutzer aktiviert sein](#)
- [\[IAM.21\] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen](#)
- [\[IAM.22\] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden](#)
- [\[IAM.23\] IAM Access Analyzer-Analysen sollten markiert werden](#)
- [\[IAM.24\] IAM-Rollen sollten mit Tags versehen werden](#)
- [\[IAM.25\] IAM-Benutzer sollten markiert werden](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[IAM.27\] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWS Cloud Shell Full Access](#)
- [\[IAM.28\] Der externe Zugriffsanalysator für IAM Access Analyzer sollte aktiviert sein](#)
- [\[Inspector.1\] Das EC2 Scannen mit Amazon Inspector sollte aktiviert sein](#)
- [\[Inspector.2\] Das Amazon Inspector ECR-Scannen sollte aktiviert sein](#)
- [\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)
- [\[Inspector.4\] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein](#)
- [\[IoT.1\] AWS IoT Device Defender Sicherheitsprofile sollten markiert werden](#)
- [\[IoT.2\] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden](#)
- [\[IoT.3\] AWS IoT Core -Dimensionen sollten markiert werden](#)
- [\[IoT.4\] AWS IoT Core Autorisierer sollten markiert werden](#)
- [\[IoT.5\] AWS IoT Core Rollenalias sollten markiert werden](#)
- [\[IoT.6\] AWS IoT Core Richtlinien sollten markiert werden](#)
- [\[IoT Events .1\] AWS IoT-Events-Eingaben sollten markiert werden](#)
- [\[IoT Events .2\] AWS IoT-Ereignisdetektormodelle sollten markiert werden](#)
- [\[IoT Events .3\] Alarmmodelle für AWS IoT Events sollten markiert werden](#)
- [\[IoT Site Wise.1\] AWS SiteWise IoT-Asset-Modelle sollten markiert werden](#)

- [\[Io TSite Wise.2\] AWS SiteWise IoT-Dashboards sollten markiert werden](#)
- [\[Io TSite Wise.3\] AWS SiteWise IoT-Gateways sollten markiert werden](#)
- [\[Io TSite Wise.4\] AWS SiteWise IoT-Portale sollten markiert werden](#)
- [\[Io TSite Wise.5\] AWS SiteWise IoT-Projekte sollten markiert werden](#)
- [\[Io TTwin Maker.1\] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden](#)
- [\[Io TTwin Maker.2\] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden](#)
- [\[Io TTwin Maker.3\] AWS TwinMaker IoT-Szenen sollten markiert werden](#)
- [\[Io TTwin Maker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[Io TWireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[Io TWireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)
- [\[Io TWireless .3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)
- [\[Keyspaces.1\] Amazon Keyspaces Keyspaces sollten mit Tags versehen sein](#)
- [\[Kinesis.1\] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden](#)
- [\[Kinesis.2\] Kinesis-Streams sollten markiert werden](#)
- [\[Kinesis.3\] Kinesis-Streams sollten über eine angemessene Aufbewahrungsfrist für Daten verfügen](#)
- [\[KMS.1\] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)
- [\[KMS.2\] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)
- [\[KMS.3\] AWS KMS keys sollte nicht unbeabsichtigt gelöscht werden](#)
- [\[KMS.5\] KMS-Schlüssel sollten nicht öffentlich zugänglich sein](#)
- [\[Lambda.5\] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren](#)
- [\[Lambda.6\] Lambda-Funktionen sollten markiert werden](#)
- [\[Lambda.7\] Bei Lambda-Funktionen sollte aktives Tracing aktiviert sein AWS X-Ray](#)
- [\[Macie.1\] Amazon Macie sollte aktiviert sein](#)
- [\[Macie.2\] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein](#)
- [\[MQ.2\] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch](#)

- [\[MQ.3\] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein](#)
- [\[MQ.4\] Amazon MQ-Broker sollten markiert werden](#)
- [\[MQ.5\] ActiveMQ-Broker sollten den Aktiv-/Standby-Bereitstellungsmodus verwenden](#)
- [\[MQ.6\] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden](#)
- [\[MSK.1\] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden](#)
- [\[MSK.2\] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein](#)
- [\[MSK.3\] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden](#)
- [\[MSK.4\] Bei MSK-Clustern sollte der öffentliche Zugriff deaktiviert sein](#)
- [\[MSK.5\] Bei MSK-Konnektoren sollte die Protokollierung aktiviert sein](#)
- [\[MSK.6\] MSK-Cluster sollten den nicht authentifizierten Zugriff deaktivieren](#)
- [\[Neptune.1\] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.2\] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)
- [\[Neptune.3\] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein](#)
- [\[Neptune.4\] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[Neptune.5\] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein](#)
- [\[Neptune.6\] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.7\] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein](#)
- [\[Neptune.8\] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren](#)
- [\[Neptune.9\] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden](#)
- [\[NetworkFirewall.1\] Network firewalls sollten über mehrere Availability Zones hinweg bereitgestellt werden](#)
- [\[NetworkFirewall.2\] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein](#)
- [\[NetworkFirewall.3\] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet haben](#)
- [\[NetworkFirewall.4\] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ sein.](#)
- [\[NetworkFirewall.5\] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ sein.](#)
- [\[NetworkFirewall.6\] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein](#)
- [\[NetworkFirewall.7\] Netzwerk-Firewall-Firewalls sollten markiert werden](#)
- [\[NetworkFirewall.8\] Firewall-Richtlinien für Netzwerk-Firewalls sollten markiert werden](#)

- [\[NetworkFirewall.9\] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein](#)
- [\[NetworkFirewall.10\] Bei Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein](#)
- [Bei \[Opensearch.1\] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein](#)
- [\[Opensearch.2\] OpenSearch -Domains sollten nicht öffentlich zugänglich sein](#)
- [\[Opensearch.3\] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden](#)
- [Die Protokollierung von \[Opensearch.4\] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein](#)
- [Für \[Opensearch.5\] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein](#)
- [\[Opensearch.6\] OpenSearch Domains sollten mindestens drei Datenknoten haben](#)
- [Für \[Opensearch.7\] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein](#)
- [\[Opensearch.8\] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden](#)
- [\[Opensearch.9\] OpenSearch -Domains sollten mit Tags versehen werden](#)
- [Auf \[Opensearch.10\] OpenSearch -Domains sollte das neueste Softwareupdate installiert sein](#)
- [\[Opensearch.11\] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben](#)
- [\[PCA.1\] AWS Private CA Root-Zertifizierungsstelle sollte deaktiviert sein](#)
- [\[PCA.2\] AWS Private CA-Zertifizierungsstellen sollten gekennzeichnet werden](#)
- [\[RDS.14\] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein](#)
- [\[RDS.16\] Aurora-DB-Cluster sollten so konfiguriert sein, dass sie Tags in DB-Snapshots kopieren](#)
- [\[RDS.17\] RDS-DB-Instances sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren](#)
- [\[RDS.18\] RDS-Instances sollten in einer VPC bereitgestellt werden](#)
- [\[RDS.19\] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Cluster-Ereignisse konfiguriert werden](#)
- [\[RDS.20\] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Ereignisse der Datenbankinstanz konfiguriert werden](#)
- [\[RDS.21\] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbankparametergruppenereignisse konfiguriert werden](#)
- [\[RDS.22\] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbanksicherheitsgruppenereignisse konfiguriert werden](#)

- [\[RDS.23\] RDS-Instances sollten keinen Standard-Port für die Datenbank-Engine verwenden](#)
- [\[RDS.24\] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden](#)
- [\[RDS.25\] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden](#)
- [\[RDS.26\] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden](#)
- [\[RDS.27\] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[RDS.28\] RDS-DB-Cluster sollten markiert werden](#)
- [\[RDS.29\] RDS-DB-Cluster-Snapshots sollten markiert werden](#)
- [\[RDS.30\] RDS-DB-Instances sollten markiert werden](#)
- [\[RDS.31\] RDS-DB-Sicherheitsgruppen sollten markiert werden](#)
- [\[RDS.32\] RDS-DB-Snapshots sollten markiert werden](#)
- [\[RDS.33\] RDS-DB-Subnetzgruppen sollten markiert werden](#)
- [\[RDS.34\] Aurora MySQL-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)
- [\[RDS.35\] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein](#)
- [\[RDS.36\] RDS für PostgreSQL-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[RDS.37\] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[RDS.38\] RDS für PostgreSQL-DB-Instances sollten bei der Übertragung verschlüsselt werden](#)
- [\[RDS.39\] RDS für MySQL-DB-Instances sollten bei der Übertragung verschlüsselt werden](#)
- [\[RDS.40\] RDS für SQL Server-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[RDS.41\] RDS für SQL Server-DB-Instances sollten bei der Übertragung verschlüsselt werden](#)
- [\[RDS.42\] RDS für MariaDB-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[RDS.44\] RDS für MariaDB-DB-Instances sollte bei der Übertragung verschlüsselt werden](#)
- [\[RDS.45\] Bei Aurora MySQL-DB-Clustern sollte die Audit-Protokollierung aktiviert sein](#)
- [\[Redshift.1\] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten](#)
- [\[Redshift.2\] Verbindungen zu Amazon Redshift Redshift-Clustern sollten bei der Übertragung verschlüsselt werden](#)
- [\[Redshift.3\] Bei Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein](#)
- [\[Redshift.4\] Bei Amazon Redshift Redshift-Clustern sollte die Auditprotokollierung aktiviert sein](#)
- [\[Redshift.6\] Bei Amazon Redshift sollten automatische Upgrades auf Hauptversionen aktiviert sein](#)
- [\[Redshift.7\] Redshift-Cluster sollten erweitertes VPC-Routing verwenden](#)

- [\[Redshift.8\] Amazon Redshift Redshift-Cluster sollten nicht den standardmäßigen Admin-Benutzernamen verwenden](#)
- [\[Redshift.9\] Redshift-Cluster sollten nicht den Standard-Datenbanknamen verwenden](#)
- [\[Redshift.10\] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[Redshift.11\] Redshift-Cluster sollten markiert werden](#)
- [\[Redshift.12\] Abonnements für Redshift-Ereignisbenachrichtigungen sollten markiert werden](#)
- [\[Redshift.13\] Redshift-Cluster-Snapshots sollten markiert werden](#)
- [\[Redshift.14\] Redshift-Cluster-Subnetzgruppen sollten markiert werden](#)
- [\[Redshift.15\] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen](#)
- [\[Redshift.16\] Redshift-Cluster-Subnetzgruppen sollten Subnetze aus mehreren Availability Zones haben](#)
- [\[Redshift.17\] Redshift-Cluster-Parametergruppen sollten markiert werden](#)
- [\[Redshift.18\] Für Redshift-Cluster sollten Multi-AZ-Bereitstellungen aktiviert sein](#)
- [\[RedshiftServerless.1\] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden](#)
- [\[RedshiftServerless.2\] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein](#)
- [\[RedshiftServerless.3\] Serverlose Redshift-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten](#)
- [\[RedshiftServerless.4\] Serverlose Redshift-Namespace sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys](#)
- [\[RedshiftServerless.5\] Redshift Serverless-Namespace sollten nicht den Standard-Admin-Benutzernamen verwenden](#)
- [\[RedshiftServerless.6\] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch](#)
- [\[RedshiftServerless.7\] Redshift Serverless-Namespace sollten nicht den Standard-Datenbanknamen verwenden](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.7\] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden](#)
- [\[S3.10\] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben](#)
- [\[S3.11\] Bei S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein](#)

- [\[S3.12\] ACLs sollte nicht zur Verwaltung des Benutzerzugriffs auf S3-Allzweck-Buckets verwendet werden](#)
- [\[S3.13\] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben](#)
- [\[S3.19\] Bei S3-Zugriffspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.20\] Bei S3-Allzweck-Buckets sollte MFA Delete aktiviert sein](#)
- [\[S3.22\] S3-Allzweck-Buckets sollten Schreibereignisse auf Objektebene protokollieren](#)
- [\[S3.23\] S3-Allzweck-Buckets sollten Leseereignisse auf Objektebene protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)
- [\[SageMaker.1\] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben](#)
- [\[SageMaker.2\] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden](#)
- [\[SageMaker.3\] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben](#)
- [\[SageMaker.4\] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein](#)
- [\[SageMaker.5\] SageMaker Modelle sollten eingehenden Datenverkehr blockieren](#)
- [\[SageMaker.6\] SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden](#)
- [\[SageMaker.7\] SageMaker Bilder sollten mit Tags versehen werden](#)
- [\[SageMaker.8\] SageMaker Notebook-Instances sollten auf unterstützten Plattformen laufen](#)
- [\[SES.1\] SES-Kontaktlisten sollten mit Tags versehen werden](#)
- [\[SES.2\] SES-Konfigurationssätze sollten mit Tags versehen werden](#)
- [\[SecretsManager.1\] Bei Secrets Manager Manager-Geheimnissen sollte die automatische Rotation aktiviert sein](#)
- [\[SecretsManager.2\] Secrets Manager Manager-Geheimnisse, die mit automatischer Rotation konfiguriert sind, sollten erfolgreich rotieren](#)
- [\[SecretsManager.3\] Unbenutzte Secrets Manager Manager-Geheimnisse entfernen](#)
- [\[SecretsManager.4\] Secrets Manager Manager-Geheimnisse sollten innerhalb einer bestimmten Anzahl von Tagen rotiert werden](#)
- [\[SecretsManager.5\] Secrets Manager Manager-Geheimnisse sollten markiert werden](#)

- [\[ServiceCatalog.1\] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden](#)
- [\[SNS.3\] SNS-Themen sollten markiert werden](#)
- [\[SNS.4\] Zugriffsrichtlinien für SNS-Themen sollten keinen öffentlichen Zugriff zulassen](#)
- [\[SQS.1\] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt werden](#)
- [\[SQS.2\] SQS-Warteschlangen sollten markiert werden](#)
- [\[SQS.3\] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen](#)
- [\[SSM.3\] Von Systems Manager verwaltete EC2 Amazon-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben](#)
- [\[SSM.4\] SSM-Dokumente sollten nicht öffentlich sein](#)
- [\[SSM.5\] SSM-Dokumente sollten mit Tags versehen werden](#)
- [\[SSM.6\] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[SSM.7\] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein](#)
- [\[StepFunctions.1\] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben](#)
- [\[StepFunctions.2\] Die Aktivitäten von Step Functions sollten mit Tags versehen werden](#)
- [\[Transfer.1\] AWS Transfer Family -Workflows sollten mit Tags versehen werden](#)
- [\[Transfer.2\] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden](#)
- [\[Transfer.3\] Bei Connectoren der Transfer-Familie sollte die Protokollierung aktiviert sein](#)
- [\[Transfer.4\] Transfer Family Familienverträge sollten gekennzeichnet werden](#)
- [\[Transfer.5\] Transfer Family Familienzertifikate sollten gekennzeichnet sein](#)
- [\[Transfer.6\] Steckverbinder der Transfer-Familie sollten gekennzeichnet sein](#)
- [\[Transfer.7\] Familienprofile sollten mit Tags versehen werden](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.2\] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.3\] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.4\] AWS WAF Classic Regional Web ACLs sollte mindestens eine Regel oder Regelgruppe enthalten](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)

- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WAF.10\] AWS WAF web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WAF.11\] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein](#)
- [Für \[WAF.12\] AWS WAF Regeln sollten Metriken aktiviert sein CloudWatch](#)
- [\[WorkSpaces.1\] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden](#)
- [\[WorkSpaces.2\] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden](#)

Naher Osten (Bahrain)

Die folgenden Steuerelemente werden in der Region Naher Osten (Bahrain) nicht unterstützt.

- [\[AppFlow.1\] AppFlow Amazon-Datenflüsse sollten mit Tags versehen werden](#)
- [\[AppRunner.1\] App Runner-Dienste sollten markiert sein](#)
- [\[AppRunner.2\] App Runner VPC-Konnektoren sollten markiert sein](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)

- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[CloudTrail.10\] Event-Datenspeicher in CloudTrail Lake sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys](#)
- [\[CodeArtifact.1\] CodeArtifact Repositorien sollten mit Tags versehen werden](#)
- [\[CodeGuruProfiler.1\] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden](#)
- [\[CodeGuruReviewer.1\] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden](#)
- [\[Connect.1\] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden](#)
- [\[Connect.2\] Für Amazon Connect Connect-Instances sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[DocumentDB.1\] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DocumentDB.2\] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen](#)
- [\[DocumentDB.3\] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein](#)
- [\[DocumentDB.4\] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch](#)
- [\[DocumentDB.5\] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[DocumentDB.6\] Amazon DocumentDB-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[DynamoDB.3\] DynamoDB Accelerator \(DAX\) -Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DynamoDB.7\] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[EC2.20\] Beide VPN-Tunnel für eine AWS Site-to-Site VPN-Verbindung sollten aktiv sein](#)
- [\[EC2.24\] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden](#)
- [\[EC2.58\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert sein](#)
- [\[EC2.60\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[ECR.4\] Öffentliche ECR-Repositorien sollten markiert werden](#)

- [\[ECR.5\] ECR-Repositorys sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys](#)
- [\[ECS.17\] ECS-Aufgabendefinitionen sollten nicht den Host-Netzwerkmodus verwenden](#)
- [\[ELB.17\] Anwendungs- und Netzwerk-Load-Balancer mit Listnern sollten die empfohlenen Sicherheitsrichtlinien verwenden](#)
- [\[EventBridge.4\] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[FSx.3\] FSx für OpenZFS-Dateisysteme sollte für die Multi-AZ-Bereitstellung konfiguriert werden](#)
- [\[FSx.4\] FSx für NetApp ONTAP-Dateisysteme sollte für die Multi-AZ-Bereitstellung konfiguriert sein](#)
- [\[FSx.5\] FSx für Windows-Dateiserver sollten für die Multi-AZ-Bereitstellung konfiguriert sein](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[Glue.4\] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue](#)
- [\[GuardDuty.11\] GuardDuty Runtime Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.12\] GuardDuty ECS Runtime Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.13\] GuardDuty EC2 Runtime Monitoring sollte aktiviert sein](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)
- [\[IoTEvents.1\] AWS IoT-Events-Eingaben sollten markiert werden](#)
- [\[IoTEvents.2\] AWS IoT-Ereignisdetektormodelle sollten markiert werden](#)
- [\[IoTEvents.3\] Alarmmodelle für AWS IoT Events sollten markiert werden](#)
- [\[IoTSiteWise.1\] AWS SiteWise IoT-Asset-Modelle sollten markiert werden](#)
- [\[IoTSiteWise.2\] AWS SiteWise IoT-Dashboards sollten markiert werden](#)
- [\[IoTSiteWise.3\] AWS SiteWise IoT-Gateways sollten markiert werden](#)
- [\[IoTSiteWise.4\] AWS SiteWise IoT-Portale sollten markiert werden](#)
- [\[IoTSiteWise.5\] AWS SiteWise IoT-Projekte sollten markiert werden](#)
- [\[IoT Twin Maker.1\] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden](#)
- [\[IoT Twin Maker.2\] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden](#)

- [\[Io TTwin Maker.3\] AWS TwinMaker IoT-Szenen sollten markiert werden](#)
- [\[Io TTwin Maker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[Io TWireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[Io TWireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)
- [\[Io TWireless .3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)
- [\[MSK.3\] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden](#)
- [\[MSK.5\] Bei MSK-Konnektoren sollte die Protokollierung aktiviert sein](#)
- [\[NetworkFirewall.10\] Bei Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein](#)
- [\[RDS.14\] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein](#)
- [\[RDS.31\] RDS-DB-Sicherheitsgruppen sollten markiert werden](#)
- [\[RDS.41\] RDS für SQL Server-DB-Instances sollten bei der Übertragung verschlüsselt werden](#)
- [\[RDS.42\] RDS für MariaDB-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch](#)
- [\[RDS.44\] RDS für MariaDB-DB-Instances sollte bei der Übertragung verschlüsselt werden](#)
- [\[RDS.45\] Bei Aurora MySQL-DB-Clustern sollte die Audit-Protokollierung aktiviert sein](#)
- [\[RedshiftServerless.1\] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden](#)
- [\[RedshiftServerless.2\] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein](#)
- [\[RedshiftServerless.3\] Serverlose Redshift-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten](#)
- [\[RedshiftServerless.4\] Serverlose Redshift-Namespaces sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys](#)
- [\[RedshiftServerless.5\] Redshift Serverless-Namespaces sollten nicht den Standard-Admin-Benutzernamen verwenden](#)
- [\[RedshiftServerless.6\] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch](#)
- [\[RedshiftServerless.7\] Redshift Serverless-Namespaces sollten nicht den Standard-Datenbanknamen verwenden](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)

- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)
- [\[SageMaker.8\] SageMaker Notebook-Instances sollten auf unterstützten Plattformen laufen](#)
- [\[SQS.3\] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen](#)
- [\[Transfer.3\] Bei Connectoren der Transfer-Familie sollte die Protokollierung aktiviert sein](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WorkSpaces.1\] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden](#)
- [\[WorkSpaces.2\] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden](#)

Naher Osten (VAE)

Die folgenden Steuerelemente werden in der Region Naher Osten (VAE) nicht unterstützt.

- [\[APIGateway.8\] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben](#)
- [\[APIGateway.9\] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein](#)
- [\[Amplify.1\] Amplify-Apps sollten markiert werden](#)
- [\[Amplify.2\] Amplify-Zweige sollten markiert werden](#)
- [\[AppConfig.1\] AWS AppConfig Anwendungen sollten markiert werden](#)
- [\[AppConfig.2\] AWS AppConfig Konfigurationsprofile sollten mit Tags versehen werden](#)
- [\[AppConfig.3\] AWS AppConfig Umgebungen sollten markiert werden](#)
- [\[AppFlow.1\] AppFlow Amazon-Datenflüsse sollten mit Tags versehen werden](#)
- [\[AppRunner.1\] App Runner-Dienste sollten markiert sein](#)
- [\[AppRunner.2\] App Runner VPC-Konnektoren sollten markiert sein](#)
- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)

- [\[AutoScaling.1\] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden](#)
- [\[Backup.1\] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein](#)
- [\[Backup.4\] AWS Backup Berichtspläne sollten markiert werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[CloudTrail.1\] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst](#)
- [\[CloudTrail.6\] Sicherstellen, dass der S3-Bucket, in dem CloudTrail Protokolle gespeichert werden, nicht öffentlich zugänglich ist](#)
- [\[CloudWatch.16\] CloudWatch Protokollgruppen sollten für einen bestimmten Zeitraum aufbewahrt werden](#)
- [\[CodeArtifact.1\] CodeArtifact Repositorien sollten mit Tags versehen werden](#)
- [\[CodeGuruProfiler.1\] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden](#)
- [\[CodeGuruReviewer.1\] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden](#)

- [\[Cognito.1\] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein](#)
- [\[Cognito.2\] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen](#)
- [\[Connect.1\] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden](#)
- [\[Connect.2\] Für Amazon Connect Connect-Instances sollte die Protokollierung aktiviert sein](#)
[CloudWatch](#)
- [\[Detective.1\] Verhaltensdiagramme von Detektiven sollten markiert werden](#)
- [\[DMS.2\] DMS-Zertifikate sollten gekennzeichnet sein](#)
- [\[DMS.3\] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden](#)
- [\[DMS.4\] DMS-Replikationsinstanzen sollten markiert werden](#)
- [\[DMS.5\] Subnetzgruppen für die DMS-Replikation sollten markiert werden](#)
- [\[DMS.6\] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein](#)
- [\[DMS.7\] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.8\] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.9\] DMS-Endpunkte sollten SSL verwenden](#)
- [\[DMS.10\] Bei DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein](#)
- [\[DMS.11\] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein](#)
- [\[DMS.12\] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein](#)
- [\[DynamoDB.3\] DynamoDB Accelerator \(DAX\) -Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DynamoDB.4\] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein](#)
- [\[DynamoDB.7\] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[EC2.4\] Gestoppte EC2 Instances sollten nach einem bestimmten Zeitraum entfernt werden](#)
- [\[EC2.8\] EC2 Instances sollten Instance Metadata Service Version 2 \(\) verwenden IMDSv2](#)
- [\[EC2.12\] Unbenutztes Amazon EC2 EIPs sollte entfernt werden](#)
- [\[EC2.14\] Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 oder: :/0 auf Port 3389 zulassen](#)
- [\[EC2.22\] Ungenutzte EC2 Amazon-Sicherheitsgruppen sollten entfernt werden](#)

- [\[EC2.24\] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden](#)
- [\[EC2.25\] EC2 Amazon-Startvorlagen sollten Netzwerkschnittstellen nicht öffentlich IPs zuweisen](#)
- [\[EC2.28\] EBS-Volumes sollten durch einen Backup-Plan abgedeckt sein](#)
- [\[EC2.51\] EC2 Client-VPN-Endpunkte sollten die Client-Verbindungsprotokollierung aktiviert haben](#)
- [\[EC2.58\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert sein](#)
- [\[EC2.60\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden](#)
- [\[EC2.170\] EC2 Startvorlagen sollten Instance Metadata Service Version 2 \(\) verwenden IMDSv2](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[EC2.175\] EC2 Startvorlagen sollten mit Tags versehen sein](#)
- [\[EC2.177\] EC2 Traffic Mirror-Sitzungen sollten mit Tags versehen werden](#)
- [\[EC2.179\] EC2 Traffic-Spiegel-Ziele sollten markiert werden](#)
- [\[EC2.180\] Bei EC2 Netzwerkschnittstellen sollte die source/destination Überprüfung aktiviert sein](#)
- [\[ECR.4\] Öffentliche ECR-Repositoryn sollten markiert werden](#)
- [\[ECS.1\] Amazon ECS-Aufgabendefinitionen sollten sichere Netzwerkmodi und Benutzerdefinitionen enthalten](#)
- [\[EFS.1\] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS](#)
- [\[EFS.2\] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein](#)
- [\[ELB.3\] Classic Load Balancer Balancer-Listener sollten mit HTTPS- oder TLS-Terminierung konfiguriert werden](#)
- [\[ELB.14\] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden](#)
- [\[ELB.17\] Anwendungs- und Netzwerk-Load-Balancer mit Listnern sollten die empfohlenen Sicherheitsrichtlinien verwenden](#)
- [\[ELB.18\] Anwendungs- und Network Load Balancer Balancer-Listener sollten sichere Protokolle verwenden, um Daten während der Übertragung zu verschlüsseln](#)
- [Bei \[ElastiCache.1\] ElastiCache \(Redis OSS\) -Clustern sollten automatische Backups aktiviert sein](#)
- [\[ElastiCache.2\] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein](#)

- [\[ElastiCache.3\] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein](#)
- [\[ElastiCache.4\] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden](#)
- [\[ElastiCache.5\] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden](#)
- [\[ElastiCache.6\] Für Replikationsgruppen ElastiCache \(Redis OSS\) früherer Versionen sollte Redis OSS AUTH aktiviert sein](#)
- [\[ElastiCache.7\] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden](#)
- [\[ElasticBeanstalk.1\] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben](#)
- [\[ElasticBeanstalk.2\] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk sollte Logs streamen nach CloudWatch](#)
- [\[EMR.1\] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben](#)
- [\[EventBridge.4\] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[Glue.4\] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue](#)
- [\[GuardDuty.2\] GuardDuty Filter sollten mit Tags versehen sein](#)
- [\[IAM.1\] IAM-Richtlinien sollten keine vollen „*“-Administratorrechte zulassen](#)
- [\[IAM.2\] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein](#)
- [\[IAM.3\] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden](#)
- [\[IAM.4\] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren](#)
- [\[IAM.5\] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen](#)
- [\[IAM.6\] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.](#)
- [\[IAM.8\] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden](#)
- [\[IAM.9\] MFA sollte für den Root-Benutzer aktiviert sein](#)
- [\[IAM.18\] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS -Support](#)

- [\[IAM.19\] MFA sollte für alle IAM-Benutzer aktiviert sein](#)
- [\[IAM.21\] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen](#)
- [\[IAM.22\] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden](#)
- [\[IAM.24\] IAM-Rollen sollten mit Tags versehen werden](#)
- [\[IAM.25\] IAM-Benutzer sollten markiert werden](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[IAM.27\] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWS Cloud Shell Full Access](#)
- [\[Inspector.1\] Das EC2 Scannen mit Amazon Inspector sollte aktiviert sein](#)
- [\[Inspector.2\] Das Amazon Inspector ECR-Scannen sollte aktiviert sein](#)
- [\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)
- [\[Inspector.4\] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein](#)
- [\[IoT Events .1\] AWS IoT-Events-Eingaben sollten markiert werden](#)
- [\[IoT Events .2\] AWS IoT-Ereignisdetektormodelle sollten markiert werden](#)
- [\[IoT Events .3\] Alarmmodelle für AWS IoT Events sollten markiert werden](#)
- [\[IoT Site Wise.1\] AWS SiteWise IoT-Asset-Modelle sollten markiert werden](#)
- [\[IoT Site Wise.2\] AWS SiteWise IoT-Dashboards sollten markiert werden](#)
- [\[IoT Site Wise.3\] AWS SiteWise IoT-Gateways sollten markiert werden](#)
- [\[IoT Site Wise.4\] AWS SiteWise IoT-Portale sollten markiert werden](#)
- [\[IoT Site Wise.5\] AWS SiteWise IoT-Projekte sollten markiert werden](#)
- [\[IoT Twin Maker.1\] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden](#)
- [\[IoT Twin Maker.2\] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden](#)
- [\[IoT Twin Maker.3\] AWS TwinMaker IoT-Szenen sollten markiert werden](#)
- [\[IoT Twin Maker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[IoT Wireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[IoT Wireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)
- [\[IoT Wireless .3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)

- [\[Keyspaces.1\] Amazon Keyspaces Keyspaces sollten mit Tags versehen sein](#)
- [\[KMS.1\] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)
- [\[KMS.2\] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen](#)
- [\[KMS.4\] Die AWS KMS Schlüsselrotation sollte aktiviert sein](#)
- [\[Lambda.7\] Bei Lambda-Funktionen sollte aktives Tracing aktiviert sein AWS X-Ray](#)
- [\[Macie.1\] Amazon Macie sollte aktiviert sein](#)
- [\[Macie.2\] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein](#)
- [\[MSK.3\] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden](#)
- [\[MSK.4\] Bei MSK-Clustern sollte der öffentliche Zugriff deaktiviert sein](#)
- [\[MSK.5\] Bei MSK-Konnektoren sollte die Protokollierung aktiviert sein](#)
- [\[MSK.6\] MSK-Cluster sollten den nicht authentifizierten Zugriff deaktivieren](#)
- [Bei \[Opensearch.1\] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein](#)
- [\[Opensearch.2\] OpenSearch -Domains sollten nicht öffentlich zugänglich sein](#)
- [\[Opensearch.3\] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden](#)
- [Die Protokollierung von \[Opensearch.4\] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein](#)
- [Für \[Opensearch.5\] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein](#)
- [\[Opensearch.6\] OpenSearch Domains sollten mindestens drei Datenknoten haben](#)
- [Für \[Opensearch.7\] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein](#)
- [\[Opensearch.8\] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden](#)
- [\[Opensearch.9\] OpenSearch -Domains sollten mit Tags versehen werden](#)
- [Auf \[Opensearch.10\] OpenSearch -Domains sollte das neueste Softwareupdate installiert sein](#)
- [\[Opensearch.11\] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben](#)
- [\[RDS.14\] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein](#)
- [\[RDS.26\] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden](#)
- [\[RDS.31\] RDS-DB-Sicherheitsgruppen sollten markiert werden](#)

- [\[RDS.35\] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein](#)
- [\[Redshift.18\] Für Redshift-Cluster sollten Multi-AZ-Bereitstellungen aktiviert sein](#)
- [\[RedshiftServerless.1\] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden](#)
- [\[RedshiftServerless.2\] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)
- [\[SageMaker.1\] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben](#)
- [\[SageMaker.2\] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden](#)
- [\[SageMaker.3\] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben](#)
- [\[SageMaker.5\] SageMaker Modelle sollten eingehenden Datenverkehr blockieren](#)
- [\[SES.1\] SES-Kontaktlisten sollten mit Tags versehen werden](#)
- [\[SES.2\] SES-Konfigurationssätze sollten mit Tags versehen werden](#)
- [\[SQS.1\] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt werden](#)
- [\[SQS.2\] SQS-Warteschlangen sollten markiert werden](#)
- [\[SQS.3\] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen](#)
- [\[SSM.1\] EC2 Amazon-Instances sollten verwaltet werden von AWS Systems Manager](#)
- [\[SSM.6\] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[SSM.7\] Bei SSM-Dokumenten sollte die Einstellung „Öffentliches Teilen blockieren“ aktiviert sein](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.3\] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)

- [\[WAF.10\] AWS WAF web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WAF.11\] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WorkSpaces.1\] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden](#)
- [\[WorkSpaces.2\] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden](#)

Südamerika (São Paulo)

Die folgenden Steuerelemente werden in der Region Südamerika (São Paulo) nicht unterstützt.

- [\[AppRunner.1\] App Runner-Dienste sollten markiert sein](#)
- [\[AppRunner.2\] App Runner VPC-Konnektoren sollten markiert sein](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[CodeArtifact.1\] CodeArtifact Repositorien sollten mit Tags versehen werden](#)
- [\[CodeGuruProfiler.1\] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden](#)
- [\[CodeGuruReviewer.1\] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden](#)

- [\[Connect.1\] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden](#)
- [\[Connect.2\] Für Amazon Connect Connect-Instances sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[ECR.4\] Öffentliche ECR-Repositoryn sollten markiert werden](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)
- [\[IoT.1\] AWS IoT Device Defender Sicherheitsprofile sollten markiert werden](#)
- [\[IoT.2\] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden](#)
- [\[IoT.3\] AWS IoT Core -Dimensionen sollten markiert werden](#)
- [\[IoTEvents .1\] AWS IoT-Events-Eingaben sollten markiert werden](#)
- [\[IoTEvents .2\] AWS IoT-Ereignisdetektormodelle sollten markiert werden](#)
- [\[IoTEvents .3\] Alarmmodelle für AWS IoT Events sollten markiert werden](#)
- [\[IoTSiteWise.1\] AWS SiteWise IoT-Asset-Modelle sollten markiert werden](#)
- [\[IoTSiteWise.2\] AWS SiteWise IoT-Dashboards sollten markiert werden](#)
- [\[IoTSiteWise.3\] AWS SiteWise IoT-Gateways sollten markiert werden](#)
- [\[IoTSiteWise.4\] AWS SiteWise IoT-Portale sollten markiert werden](#)
- [\[IoTSiteWise.5\] AWS SiteWise IoT-Projekte sollten markiert werden](#)
- [\[IoT Twin Maker.1\] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden](#)
- [\[IoT Twin Maker.2\] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden](#)
- [\[IoT Twin Maker.3\] AWS TwinMaker IoT-Szenen sollten markiert werden](#)
- [\[IoT Twin Maker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)

- [\[RDS.14\] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein](#)
- [\[RedshiftServerless.1\] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden](#)
- [\[RedshiftServerless.2\] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)

AWS GovCloud (US-Ost)

Die folgenden Steuerelemente werden in der Region AWS GovCloud (USA-Ost) nicht unterstützt.

- [\[ACM.2\] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden](#)
- [\[Account.1\] Sicherheitskontaktinformationen sollten bereitgestellt werden für AWS-Konto](#)
- [\[Account.2\] AWS-Konten sollte Teil einer Organisation sein AWS Organizations](#)
- [\[APIGateway.2\] API Gateway REST API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden](#)
- [\[APIGateway.8\] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben](#)
- [\[APIGateway.9\] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein](#)
- [\[Amplify.1\] Amplify-Apps sollten markiert werden](#)
- [\[Amplify.2\] Amplify-Zweige sollten markiert werden](#)
- [\[AppConfig.1\] AWS AppConfig Anwendungen sollten markiert werden](#)
- [\[AppConfig.2\] AWS AppConfig Konfigurationsprofile sollten mit Tags versehen werden](#)
- [\[AppConfig.3\] AWS AppConfig Umgebungen sollten markiert werden](#)

- [\[AppConfig.4\] AWS AppConfig Erweiterungszuordnungen sollten markiert werden](#)
- [\[AppFlow.1\] AppFlow Amazon-Datenflüsse sollten mit Tags versehen werden](#)
- [\[AppRunner.1\] App Runner-Dienste sollten markiert sein](#)
- [\[AppRunner.2\] App Runner VPC-Konnektoren sollten markiert sein](#)
- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.2\] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben](#)
- [\[AppSync.4\] AWS AppSync GraphQL APIs sollte markiert sein](#)
- [\[AppSync.5\] AWS AppSync GraphQL APIs sollte nicht mit API-Schlüsseln authentifiziert werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [\[AutoScaling.2\] Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken](#)
- [\[AutoScaling.3\] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2 Instances so konfigurieren, dass sie Instance Metadata Service Version 2 \(IMDSv2\) benötigen](#)
- [\[AutoScaling.6\] Auto Scaling Scaling-Gruppen sollten mehrere Instance-Typen in mehreren Availability Zones verwenden](#)
- [\[AutoScaling.9\] Amazon EC2 Auto Scaling Scaling-Gruppen sollten EC2 Amazon-Startvorlagen verwenden](#)
- [\[Backup.4\] AWS Backup Berichtspläne sollten markiert werden](#)
- [\[Batch.1\] Warteschlangen für Batch-Jobs sollten markiert werden](#)
- [\[Batch.2\] Richtlinien für die Batch-Planung sollten gekennzeichnet sein](#)
- [\[Batch.3\] Batch-Computing-Umgebungen sollten markiert werden](#)
- [\[Batch.4\] Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)
- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)

- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[CloudWatch.17\] CloudWatch Alarmaktionen sollten aktiviert sein](#)
- [\[CodeArtifact.1\] CodeArtifact Repositorien sollten mit Tags versehen werden](#)
- [\[CodeBuild.3\] CodeBuild S3-Protokolle sollten verschlüsselt sein](#)
- [\[CodeBuild.4\] CodeBuild Projektumgebungen sollten eine AWS Config Protokollierungsdauer haben](#)
- [\[CodeGuruProfiler.1\] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden](#)
- [\[CodeGuruReviewer.1\] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden](#)
- [\[Cognito.1\] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein](#)
- [\[Cognito.2\] Cognito-Identitätspools sollten keine nicht authentifizierten Identitäten zulassen](#)
- [\[Connect.1\] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden](#)
- [\[Connect.2\] Für Amazon Connect Connect-Instances sollte die Protokollierung aktiviert sein](#)
[CloudWatch](#)
- [\[DataSync.2\] DataSync Aufgaben sollten mit Tags versehen werden](#)
- [\[DMS.2\] DMS-Zertifikate sollten gekennzeichnet sein](#)
- [\[DMS.6\] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein](#)
- [\[DMS.7\] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.8\] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.9\] DMS-Endpunkte sollten SSL verwenden](#)

- [\[DocumentDB.1\] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DocumentDB.2\] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen](#)
- [\[DocumentDB.3\] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein](#)
- [\[DocumentDB.4\] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch](#)
- [\[DocumentDB.5\] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[DynamoDB.3\] DynamoDB Accelerator \(DAX\) -Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DynamoDB.7\] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[EC2.21\] Das Netzwerk ACLs sollte keinen Zugang von 0.0.0.0/0 zu Port 22 oder Port 3389 zulassen](#)
- [\[EC2.22\] Ungenutzte EC2 Amazon-Sicherheitsgruppen sollten entfernt werden](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways sollte VPC-Anhangsanfragen nicht automatisch akzeptieren](#)
- [\[EC2.24\] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden](#)
- [\[EC2.25\] EC2 Amazon-Startvorlagen sollten Netzwerkschnittstellen nicht öffentlich IPs zuweisen](#)
- [\[EC2.47\] Amazon VPC Endpoint Services sollten markiert werden](#)
- [\[EC2.52\] EC2 Transit-Gateways sollten markiert werden](#)
- [\[EC2.58\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert sein](#)
- [\[EC2.60\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden](#)
- [\[EC2.170\] EC2 Startvorlagen sollten Instance Metadata Service Version 2 \(\) verwenden IMDSv2](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)
- [\[EC2.174\] EC2 DHCP-Optionssätze sollten mit Tags versehen werden](#)
- [\[EC2.175\] EC2 Startvorlagen sollten mit Tags versehen sein](#)
- [\[EC2.176\] EC2 Präfixlisten sollten mit Tags versehen werden](#)
- [\[EC2.177\] EC2 Traffic Mirror-Sitzungen sollten mit Tags versehen werden](#)
- [\[EC2.178\] Filter für EC2 Verkehrsspiegel sollten mit Tags versehen werden](#)

- [\[EC2.179\] EC2 Traffic-Spiegel-Ziele sollten markiert werden](#)
- [\[ECR.1\] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein](#)
- [\[ECR.2\] Bei privaten ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein](#)
- [\[ECR.3\] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein](#)
- [\[ECR.4\] Öffentliche ECR-Repositoryn sollten markiert werden](#)
- [\[ECS.3\] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen](#)
- [\[ECS.4\] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden](#)
- [\[ECS.5\] ECS-Container sollten auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sein](#)
- [\[ECS.8\] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden](#)
- [\[ECS.9\] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen](#)
- [\[ECS.10\] Die ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen](#)
- [\[ECS.12\] ECS-Cluster sollten Container Insights verwenden](#)
- [\[EFS.3\] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen](#)
- [\[EFS.4\] EFS-Zugangspunkte sollten eine Benutzeridentität erzwingen](#)
- [\[EKS.2\] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden](#)
- [\[EKS.8\] Bei EKS-Clustern sollte die Auditprotokollierung aktiviert sein](#)
- [\[ELB.10\] Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken](#)
- [\[ELB.12\] Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden](#)
- [\[ELB.13\] Anwendungs-, Netzwerk- und Gateway-Load Balancer sollten sich über mehrere Availability Zones erstrecken](#)
- [\[ELB.14\] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden](#)
- [\[ELB.16\] Application Load Balancers sollten mit einer Web-ACL verknüpft sein AWS WAF](#)
- [Bei \[ElastiCache.1\] ElastiCache \(Redis OSS\) -Clustern sollten automatische Backups aktiviert sein](#)
- [\[ElastiCache.2\] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein](#)
- [\[ElastiCache.3\] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein](#)
- [\[ElastiCache.4\] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden](#)

- [\[ElastiCache.5\] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden](#)
- [\[ElastiCache.6\] Für Replikationsgruppen ElastiCache \(Redis OSS\) früherer Versionen sollte Redis OSS AUTH aktiviert sein](#)
- [\[ElastiCache.7\] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden](#)
- [\[ElasticBeanstalk.1\] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben](#)
- [\[ElasticBeanstalk.2\] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk sollte Logs streamen nach CloudWatch](#)
- [\[EMR.2\] Die Amazon EMR-Einstellung zum Blockieren des öffentlichen Zugriffs sollte aktiviert sein](#)
- [\[EMR.3\] Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden](#)
- [\[EMR.4\] Amazon EMR-Sicherheitskonfigurationen sollten bei der Übertragung verschlüsselt werden](#)
- [\[ES.4\] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein](#)
- [\[EventBridge.3\] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden](#)
- [\[EventBridge.4\] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[FSx.1\] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden](#)
- [\[FSx.2\] FSx für Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[Glue.3\] Transformationen für AWS Glue maschinelles Lernen sollten im Ruhezustand verschlüsselt werden](#)
- [\[GuardDuty.7\] GuardDuty EKS Runtime Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.8\] Der GuardDuty Malware-Schutz für EC2 sollte aktiviert sein](#)
- [\[GuardDuty.9\] Der GuardDuty RDS-Schutz sollte aktiviert sein](#)
- [\[GuardDuty.11\] GuardDuty Runtime Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.12\] GuardDuty ECS Runtime Monitoring sollte aktiviert sein](#)

- [\[GuardDuty.13\] GuardDuty EC2 Runtime Monitoring sollte aktiviert sein](#)
- [\[IAM.6\] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.](#)
- [\[IAM.9\] MFA sollte für den Root-Benutzer aktiviert sein](#)
- [\[IAM.21\] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen](#)
- [\[IAM.24\] IAM-Rollen sollten mit Tags versehen werden](#)
- [\[IAM.25\] IAM-Benutzer sollten markiert werden](#)
- [\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden](#)
- [\[IAM.28\] Der externe Zugriffsanalysator für IAM Access Analyzer sollte aktiviert sein](#)
- [\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)
- [\[IoT TEEvents .1\] AWS IoT-Events-Eingaben sollten markiert werden](#)
- [\[IoT TEEvents .2\] AWS IoT-Ereignisdetektormodelle sollten markiert werden](#)
- [\[IoT TEEvents .3\] Alarmmodelle für AWS IoT Events sollten markiert werden](#)
- [\[IoT TSite Wise.1\] AWS SiteWise IoT-Asset-Modelle sollten markiert werden](#)
- [\[IoT TSite Wise.2\] AWS SiteWise IoT-Dashboards sollten markiert werden](#)
- [\[IoT TSite Wise.3\] AWS SiteWise IoT-Gateways sollten markiert werden](#)
- [\[IoT TSite Wise.4\] AWS SiteWise IoT-Portale sollten markiert werden](#)
- [\[IoT TSite Wise.5\] AWS SiteWise IoT-Projekte sollten markiert werden](#)
- [\[IoT TTwin Maker.1\] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden](#)
- [\[IoT TTwin Maker.2\] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden](#)
- [\[IoT TTwin Maker.3\] AWS TwinMaker IoT-Szenen sollten markiert werden](#)
- [\[IoT TTwin Maker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[IoT TWireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[IoT TWireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)
- [\[IoT TWireless .3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)
- [\[Keyspaces.1\] Amazon Keyspaces Keyspaces sollten mit Tags versehen sein](#)
- [\[Kinesis.1\] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden](#)

- [\[KMS.5\] KMS-Schlüssel sollten nicht öffentlich zugänglich sein](#)
- [\[Lambda.5\] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren](#)
- [\[Macie.1\] Amazon Macie sollte aktiviert sein](#)
- [\[Macie.2\] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein](#)
- [\[MQ.3\] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein](#)
- [\[MQ.5\] ActiveMQ-Broker sollten den Aktiv-/Standby-Bereitstellungsmodus verwenden](#)
- [\[MQ.6\] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden](#)
- [\[MSK.1\] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden](#)
- [\[MSK.2\] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein](#)
- [\[MSK.3\] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden](#)
- [\[MSK.5\] Bei MSK-Konnektoren sollte die Protokollierung aktiviert sein](#)
- [\[Neptune.1\] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.2\] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)
- [\[Neptune.3\] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein](#)
- [\[Neptune.4\] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[Neptune.5\] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein](#)
- [\[Neptune.6\] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.7\] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein](#)
- [\[Neptune.8\] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren](#)
- [\[Neptune.9\] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden](#)
- [\[NetworkFirewall.1\] Network firewalls sollten über mehrere Availability Zones hinweg bereitgestellt werden](#)
- [\[NetworkFirewall.2\] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein](#)
- [\[NetworkFirewall.3\] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet haben](#)
- [\[NetworkFirewall.4\] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ sein.](#)
- [\[NetworkFirewall.5\] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ sein.](#)
- [\[NetworkFirewall.6\] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein](#)
- [\[NetworkFirewall.9\] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein](#)

- [Bei \[Opensearch.1\] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein](#)
- [\[Opensearch.2\] OpenSearch -Domains sollten nicht öffentlich zugänglich sein](#)
- [\[Opensearch.3\] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden](#)
- [Die Protokollierung von \[Opensearch.4\] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein](#)
- [Für \[Opensearch.5\] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein](#)
- [\[Opensearch.6\] OpenSearch Domains sollten mindestens drei Datenknoten haben](#)
- [Für \[Opensearch.7\] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein](#)
- [\[Opensearch.8\] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden](#)
- [\[PCA.1\] AWS Private CA Root-Zertifizierungsstelle sollte deaktiviert sein](#)
- [\[PCA.2\] AWS Private CA-Zertifizierungsstellen sollten gekennzeichnet werden](#)
- [\[RDS.14\] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein](#)
- [\[RDS.15\] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden](#)
- [\[RDS.24\] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden](#)
- [\[RDS.25\] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden](#)
- [\[RDS.27\] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[RDS.31\] RDS-DB-Sicherheitsgruppen sollten markiert werden](#)
- [\[RDS.34\] Aurora MySQL-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)
- [\[RDS.35\] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein](#)
- [\[RDS.45\] Bei Aurora MySQL-DB-Clustern sollte die Audit-Protokollierung aktiviert sein](#)
- [\[Redshift.8\] Amazon Redshift Redshift-Cluster sollten nicht den standardmäßigen Admin-Benutzernamen verwenden](#)
- [\[Redshift.9\] Redshift-Cluster sollten nicht den Standard-Datenbanknamen verwenden](#)
- [\[Redshift.10\] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[Redshift.17\] Redshift-Cluster-Parametergruppen sollten markiert werden](#)
- [\[RedshiftServerless.1\] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden](#)

- [\[RedshiftServerless.2\] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein](#)
- [\[RedshiftServerless.3\] Serverlose Redshift-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten](#)
- [\[RedshiftServerless.6\] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.10\] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben](#)
- [\[S3.11\] Bei S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein](#)
- [\[S3.12\] ACLs sollte nicht zur Verwaltung des Benutzerzugriffs auf S3-Allzweck-Buckets verwendet werden](#)
- [\[S3.13\] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben](#)
- [\[S3.20\] Bei S3-Allzweck-Buckets sollte MFA Delete aktiviert sein](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)
- [\[SageMaker.1\] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben](#)
- [\[SageMaker.2\] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden](#)
- [\[SageMaker.3\] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben](#)
- [\[SageMaker.5\] SageMaker Modelle sollten eingehenden Datenverkehr blockieren](#)
- [\[SageMaker.6\] SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden](#)
- [\[SageMaker.7\] SageMaker Bilder sollten mit Tags versehen werden](#)
- [\[SES.1\] SES-Kontaktlisten sollten mit Tags versehen werden](#)
- [\[SES.2\] SES-Konfigurationssätze sollten mit Tags versehen werden](#)
- [\[SNS.4\] Zugriffsrichtlinien für SNS-Themen sollten keinen öffentlichen Zugriff zulassen](#)
- [\[SQS.3\] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen](#)
- [\[SSM.4\] SSM-Dokumente sollten nicht öffentlich sein](#)
- [\[SSM.5\] SSM-Dokumente sollten mit Tags versehen werden](#)

- [\[SSM.6\] Bei SSM Automation sollte die Protokollierung aktiviert sein CloudWatch](#)
- [\[StepFunctions.1\] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben](#)
- [\[StepFunctions.2\] Die Aktivitäten von Step Functions sollten mit Tags versehen werden](#)
- [\[Transfer.4\] Transfer Family Familienverträge sollten gekennzeichnet werden](#)
- [\[Transfer.5\] Transfer Family Familienzertifikate sollten gekennzeichnet sein](#)
- [\[Transfer.6\] Steckverbinder der Transfer-Familie sollten gekennzeichnet sein](#)
- [\[Transfer.7\] Familienprofile sollten mit Tags versehen werden](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.2\] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.3\] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.4\] AWS WAF Classic Regional Web ACLs sollte mindestens eine Regel oder Regelgruppe enthalten](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WAF.10\] AWS WAF web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [Für \[WAF.12\] AWS WAF Regeln sollten Metriken aktiviert sein CloudWatch](#)
- [\[WorkSpaces.1\] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden](#)
- [\[WorkSpaces.2\] WorkSpaces Root-Volumes sollten im Ruhezustand verschlüsselt werden](#)

AWS GovCloud (US-West)

Die folgenden Steuerelemente werden in der Region AWS GovCloud (US-West) nicht unterstützt.

- [\[ACM.2\] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden](#)
- [\[Account.1\] Sicherheitskontaktinformationen sollten bereitgestellt werden für AWS-Konto](#)
- [\[Account.2\] AWS-Konten sollte Teil einer Organisation sein AWS Organizations](#)
- [\[APIGateway.2\] API Gateway REST API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden](#)

- [\[APIGateway.8\] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben](#)
- [\[APIGateway.9\] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein](#)
- [\[Amplify.1\] Amplify-Apps sollten markiert werden](#)
- [\[Amplify.2\] Amplify-Zweige sollten markiert werden](#)
- [\[AppConfig.1\] AWS AppConfig Anwendungen sollten markiert werden](#)
- [\[AppConfig.2\] AWS AppConfig Konfigurationsprofile sollten mit Tags versehen werden](#)
- [\[AppConfig.3\] AWS AppConfig Umgebungen sollten markiert werden](#)
- [\[AppConfig.4\] AWS AppConfig Erweiterungsuzuordnungen sollten markiert werden](#)
- [\[AppFlow.1\] AppFlow Amazon-Datenflüsse sollten mit Tags versehen werden](#)
- [\[AppRunner.1\] App Runner-Dienste sollten markiert sein](#)
- [\[AppRunner.2\] App Runner VPC-Konnektoren sollten markiert sein](#)
- [\[AppSync.1\] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden](#)
- [\[AppSync.2\] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben](#)
- [\[AppSync.4\] AWS AppSync GraphQL APIs sollte markiert sein](#)
- [\[AppSync.5\] AWS AppSync GraphQL APIs sollte nicht mit API-Schlüsseln authentifiziert werden](#)
- [\[AppSync.6\] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden](#)
- [\[AutoScaling.2\] Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken](#)
- [\[AutoScaling.3\] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2 Instances so konfigurieren, dass sie Instance Metadata Service Version 2 \(IMDSv2\) benötigen](#)
- [\[AutoScaling.6\] Auto Scaling Scaling-Gruppen sollten mehrere Instance-Typen in mehreren Availability Zones verwenden](#)
- [\[AutoScaling.9\] Amazon EC2 Auto Scaling Scaling-Gruppen sollten EC2 Amazon-Startvorlagen verwenden](#)
- [\[Backup.4\] AWS Backup Berichtspläne sollten markiert werden](#)
- [\[Batch.1\] Warteschlangen für Batch-Jobs sollten markiert werden](#)
- [\[Batch.2\] Richtlinien für die Batch-Planung sollten gekennzeichnet sein](#)
- [\[Batch.3\] Batch-Computing-Umgebungen sollten markiert werden](#)
- [\[Batch.4\] Eigenschaften von Rechenressourcen in verwalteten Batch-Computing-Umgebungen sollten mit Tags versehen werden](#)
- [Bei \[CloudFront.1\] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein](#)

- [\[CloudFront.3\] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen](#)
- [\[CloudFront.4\] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein](#)
- [\[CloudFront.5\] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein](#)
- [\[CloudFront.6\] Bei CloudFront Distributionen sollte WAF aktiviert sein](#)
- [\[CloudFront.7\] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden](#)
- [\[CloudFront.8\] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten](#)
- [\[CloudFront.9\] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln](#)
- [\[CloudFront.10\] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden](#)
- [\[CloudFront.12\] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen](#)
- [\[CloudFront.13\] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden](#)
- [\[CloudFront.14\] CloudFront Distributionen sollten mit Tags versehen werden](#)
- [\[CloudFront.15\] CloudFront Distributionen sollten die empfohlene TLS-Sicherheitsrichtlinie verwenden](#)
- [\[CloudWatch.17\] CloudWatch Alarmaktionen sollten aktiviert sein](#)
- [\[CodeArtifact.1\] CodeArtifact Repositorien sollten mit Tags versehen werden](#)
- [\[CodeBuild.3\] CodeBuild S3-Protokolle sollten verschlüsselt sein](#)
- [\[CodeBuild1.4\] CodeBuild Projektumgebungen sollten eine AWS Config Protokollierungsdauer haben](#)
- [\[CodeGuruProfiler.1\] CodeGuru Profiler-Profiling-Gruppen sollten markiert werden](#)
- [\[CodeGuruReviewer.1\] CodeGuru Reviewer-Repository-Verknüpfungen sollten markiert werden](#)
- [\[Cognito.1\] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein](#)
- [\[Connect.1\] Objekttypen von Amazon Connect Customer Profiles sollten mit Tags versehen werden](#)
- [\[DataSync.2\] DataSync Aufgaben sollten mit Tags versehen werden](#)
- [\[DMS.2\] DMS-Zertifikate sollten gekennzeichnet sein](#)
- [\[DMS.6\] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein](#)

- [\[DMS.7\] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.8\] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein](#)
- [\[DMS.9\] DMS-Endpunkte sollten SSL verwenden](#)
- [\[DocumentDB.1\] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DocumentDB.2\] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen](#)
- [\[DocumentDB.3\] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein](#)
- [\[DocumentDB.4\] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch](#)
- [\[DocumentDB.5\] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[DynamoDB.3\] DynamoDB Accelerator \(DAX\) -Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[DynamoDB.7\] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden](#)
- [\[EC2.21\] Das Netzwerk ACLs sollte keinen Zugang von 0.0.0.0/0 zu Port 22 oder Port 3389 zulassen](#)
- [\[EC2.22\] Ungenutzte EC2 Amazon-Sicherheitsgruppen sollten entfernt werden](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways sollte VPC-Anhangsanfragen nicht automatisch akzeptieren](#)
- [\[EC2.24\] EC2 Paravirtual-Instance-Typen von Amazon sollten nicht verwendet werden](#)
- [\[EC2.25\] EC2 Amazon-Startvorlagen sollten Netzwerkschnittstellen nicht öffentlich IPs zuweisen](#)
- [\[EC2.28\] EBS-Volumes sollten durch einen Backup-Plan abgedeckt sein](#)
- [\[EC2.38\] EC2 Instances sollten markiert werden](#)
- [\[EC2.58\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager-Kontakte konfiguriert sein](#)
- [\[EC2.60\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden](#)
- [\[EC2.170\] EC2 Startvorlagen sollten Instance Metadata Service Version 2 \(\) verwenden IMDSv2](#)
- [\[EC2.173\] EC2 Spot-Flottenanfragen mit Startparametern sollten die Verschlüsselung für angehängte EBS-Volumes ermöglichen](#)

- [\[EC2.174\] EC2 DHCP-Optionssätze sollten mit Tags versehen werden](#)
- [\[EC2.175\] EC2 Startvorlagen sollten mit Tags versehen sein](#)
- [\[EC2.176\] EC2 Präfixlisten sollten mit Tags versehen werden](#)
- [\[EC2.177\] EC2 Traffic Mirror-Sitzungen sollten mit Tags versehen werden](#)
- [\[EC2.178\] Filter für EC2 Verkehrsspiegel sollten mit Tags versehen werden](#)
- [\[EC2.179\] EC2 Traffic-Spiegel-Ziele sollten markiert werden](#)
- [\[ECR.1\] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein](#)
- [\[ECR.2\] Bei privaten ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein](#)
- [\[ECR.3\] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein](#)
- [\[ECR.4\] Öffentliche ECR-Repositoryn sollten markiert werden](#)
- [\[ECS.3\] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen](#)
- [\[ECS.4\] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden](#)
- [\[ECS.5\] ECS-Container sollten auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sein](#)
- [\[ECS.8\] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden](#)
- [\[ECS.9\] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen](#)
- [\[ECS.10\] Die ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen](#)
- [\[ECS.12\] ECS-Cluster sollten Container Insights verwenden](#)
- [\[EFS.3\] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen](#)
- [\[EFS.4\] EFS-Zugangspunkte sollten eine Benutzeridentität erzwingen](#)
- [\[EKS.2\] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden](#)
- [\[EKS.8\] Bei EKS-Clustern sollte die Auditprotokollierung aktiviert sein](#)
- [\[ELB.10\] Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken](#)
- [\[ELB.12\] Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden](#)
- [\[ELB.13\] Anwendungs-, Netzwerk- und Gateway-Load Balancer sollten sich über mehrere Availability Zones erstrecken](#)
- [\[ELB.14\] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden](#)
- [\[ELB.16\] Application Load Balancers sollten mit einer Web-ACL verknüpft sein AWS WAF](#)

- [Bei \[ElastiCache.1\] ElastiCache \(Redis OSS\) -Clustern sollten automatische Backups aktiviert sein](#)
- [\[ElastiCache.2\] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein](#)
- [\[ElastiCache.3\] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein](#)
- [\[ElastiCache.4\] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden](#)
- [\[ElastiCache.5\] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden](#)
- [\[ElastiCache.6\] Für Replikationsgruppen ElastiCache \(Redis OSS\) früherer Versionen sollte Redis OSS AUTH aktiviert sein](#)
- [\[ElastiCache.7\] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden](#)
- [\[ElasticBeanstalk.1\] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben](#)
- [\[ElasticBeanstalk.2\] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk sollte Logs streamen nach CloudWatch](#)
- [\[EMR.2\] Die Amazon EMR-Einstellung zum Blockieren des öffentlichen Zugriffs sollte aktiviert sein](#)
- [\[EMR.3\] Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden](#)
- [\[EMR.4\] Amazon EMR-Sicherheitskonfigurationen sollten bei der Übertragung verschlüsselt werden](#)
- [\[ES.4\] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein](#)
- [\[EventBridge.3\] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden](#)
- [\[EventBridge.4\] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein](#)
- [\[FraudDetector.1\] Entitätstypen von Amazon Fraud Detector sollten markiert werden](#)
- [\[FraudDetector.2\] Amazon Fraud Detector Detector-Etiketten sollten gekennzeichnet sein](#)
- [\[FraudDetector.3\] Die Ergebnisse von Amazon Fraud Detector sollten gekennzeichnet werden](#)
- [\[FraudDetector.4\] Amazon Fraud Detector Detector-Variablen sollten markiert werden](#)
- [\[FSx.1\] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden](#)
- [\[FSx.2\] FSx für Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden](#)
- [\[GlobalAccelerator.1\] Global Accelerator-Beschleuniger sollten gekennzeichnet sein](#)
- [\[GuardDuty.7\] GuardDuty EKS Runtime Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.8\] Der GuardDuty Malware-Schutz für EC2 sollte aktiviert sein](#)

- [\[GuardDuty.9\] Der GuardDuty RDS-Schutz sollte aktiviert sein](#)
- [\[GuardDuty.11\] GuardDuty Runtime Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.12\] GuardDuty ECS Runtime Monitoring sollte aktiviert sein](#)
- [\[GuardDuty.13\] GuardDuty EC2 Runtime Monitoring sollte aktiviert sein](#)
- [\[IAM.6\] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.](#)
- [\[IAM.9\] MFA sollte für den Root-Benutzer aktiviert sein](#)
- [\[IAM.21\] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen](#)
- [\[IAM.24\] IAM-Rollen sollten mit Tags versehen werden](#)
- [\[IAM.25\] IAM-Benutzer sollten markiert werden](#)
- [\[IAM.28\] Der externe Zugriffsanalysator für IAM Access Analyzer sollte aktiviert sein](#)
- [\[Inspector.3\] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein](#)
- [\[IoT Events .1\] AWS IoT-Events-Eingaben sollten markiert werden](#)
- [\[IoT Events .2\] AWS IoT-Ereignisdetektormodelle sollten markiert werden](#)
- [\[IoT Events .3\] Alarmmodelle für AWS IoT Events sollten markiert werden](#)
- [\[IoT Site Wise.1\] AWS SiteWise IoT-Asset-Modelle sollten markiert werden](#)
- [\[IoT Site Wise.2\] AWS SiteWise IoT-Dashboards sollten markiert werden](#)
- [\[IoT Site Wise.3\] AWS SiteWise IoT-Gateways sollten markiert werden](#)
- [\[IoT Site Wise.4\] AWS SiteWise IoT-Portale sollten markiert werden](#)
- [\[IoT Site Wise.5\] AWS SiteWise IoT-Projekte sollten markiert werden](#)
- [\[IoT Twin Maker.1\] AWS TwinMaker IoT-Synchronisierungsjobs sollten markiert werden](#)
- [\[IoT Twin Maker.2\] AWS TwinMaker IoT-Arbeitsbereiche sollten markiert werden](#)
- [\[IoT Twin Maker.3\] AWS TwinMaker IoT-Szenen sollten markiert werden](#)
- [\[IoT Twin Maker.4\] AWS TwinMaker IoT-Entitäten sollten markiert werden](#)
- [\[IoT Wireless .1\] AWS IoT Wireless Wireless-Multicast-Gruppen sollten markiert werden](#)
- [\[IoT Wireless .2\] AWS IoT-Wireless-Dienstprofile sollten markiert werden](#)
- [\[IoT Wireless .3\] AWS IoT FUOTA-Aufgaben sollten markiert werden](#)
- [\[IVS.1\] Schlüsselpaare für die IVS-Wiedergabe sollten markiert sein](#)
- [\[IVS.2\] IVS-Aufzeichnungskonfigurationen sollten markiert werden](#)
- [\[IVS.3\] IVS-Kanäle sollten markiert werden](#)
- [\[Keyspaces.1\] Amazon Keyspaces Keyspaces sollten mit Tags versehen sein](#)

- [\[Kinesis.1\] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden](#)
- [\[KMS.5\] KMS-Schlüssel sollten nicht öffentlich zugänglich sein](#)
- [\[Lambda.5\] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren](#)
- [\[Macie.1\] Amazon Macie sollte aktiviert sein](#)
- [\[Macie.2\] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein](#)
- [\[MQ.3\] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein](#)
- [\[MQ.5\] ActiveMQ-Broker sollten den Aktiv-/Standby-Bereitstellungsmodus verwenden](#)
- [\[MQ.6\] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden](#)
- [\[MSK.1\] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden](#)
- [\[MSK.2\] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein](#)
- [\[MSK.3\] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden](#)
- [\[MSK.5\] Bei MSK-Konnektoren sollte die Protokollierung aktiviert sein](#)
- [\[Neptune.1\] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.2\] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)
- [\[Neptune.3\] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein](#)
- [\[Neptune.4\] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein](#)
- [\[Neptune.5\] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein](#)
- [\[Neptune.6\] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden](#)
- [\[Neptune.7\] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein](#)
- [\[Neptune.8\] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren](#)
- [\[Neptune.9\] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden](#)
- [\[NetworkFirewall.1\] Network firewalls sollten über mehrere Availability Zones hinweg bereitgestellt werden](#)
- [\[NetworkFirewall.2\] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein](#)
- [\[NetworkFirewall.3\] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet haben](#)
- [\[NetworkFirewall.4\] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ sein.](#)
- [\[NetworkFirewall.5\] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ sein.](#)
- [\[NetworkFirewall.6\] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein](#)

- [\[NetworkFirewall.9\] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein](#)
- [Bei \[Opensearch.1\] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein](#)
- [\[Opensearch.2\] OpenSearch -Domains sollten nicht öffentlich zugänglich sein](#)
- [\[Opensearch.3\] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden](#)
- [Die Protokollierung von \[Opensearch.4\] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein](#)
- [Für \[Opensearch.5\] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein](#)
- [\[Opensearch.6\] OpenSearch Domains sollten mindestens drei Datenknoten haben](#)
- [Für \[Opensearch.7\] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein](#)
- [\[Opensearch.8\] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden](#)
- [\[PCA.1\] AWS Private CA Root-Zertifizierungsstelle sollte deaktiviert sein](#)
- [\[PCA.2\] AWS Private CA-Zertifizierungsstellen sollten gekennzeichnet werden](#)
- [\[RDS.14\] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein](#)
- [\[RDS.15\] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden](#)
- [\[RDS.24\] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden](#)
- [\[RDS.25\] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden](#)
- [\[RDS.27\] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[RDS.34\] Aurora MySQL-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch](#)
- [\[RDS.35\] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein](#)
- [\[RDS.45\] Bei Aurora MySQL-DB-Clustern sollte die Audit-Protokollierung aktiviert sein](#)
- [\[Redshift.7\] Redshift-Cluster sollten erweitertes VPC-Routing verwenden](#)
- [\[Redshift.8\] Amazon Redshift Redshift-Cluster sollten nicht den standardmäßigen Admin-Benutzernamen verwenden](#)
- [\[Redshift.9\] Redshift-Cluster sollten nicht den Standard-Datenbanknamen verwenden](#)
- [\[Redshift.10\] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden](#)
- [\[Redshift.11\] Redshift-Cluster sollten markiert werden](#)
- [\[Redshift.13\] Redshift-Cluster-Snapshots sollten markiert werden](#)

- [\[Redshift.17\] Redshift-Cluster-Parametergruppen sollten markiert werden](#)
- [\[RedshiftServerless.1\] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden](#)
- [\[RedshiftServerless.2\] Für die Verwendung von SSL sollten Verbindungen zu Redshift Serverless-Arbeitsgruppen erforderlich sein](#)
- [\[RedshiftServerless.3\] Serverlose Redshift-Arbeitsgruppen sollten den öffentlichen Zugriff verbieten](#)
- [\[RedshiftServerless.6\] Redshift Serverless Namespaces sollten Protokolle in Logs exportieren CloudWatch](#)
- [\[Route 53.1\] Route 53-Zustandsprüfungen sollten gekennzeichnet sein](#)
- [\[Route53.2\] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren](#)
- [\[S3.10\] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben](#)
- [\[S3.11\] Bei S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein](#)
- [\[S3.12\] ACLs sollte nicht zur Verwaltung des Benutzerzugriffs auf S3-Allzweck-Buckets verwendet werden](#)
- [\[S3.13\] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben](#)
- [\[S3.20\] Bei S3-Allzweck-Buckets sollte MFA Delete aktiviert sein](#)
- [\[S3.24\] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die Blockierung des öffentlichen Zugriffs aktiviert sein](#)
- [\[S3.25\] S3-Verzeichnis-Buckets sollten Lebenszykluskonfigurationen haben](#)
- [\[SageMaker.2\] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden](#)
- [\[SageMaker.3\] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben](#)
- [\[SageMaker.5\] SageMaker Modelle sollten eingehenden Datenverkehr blockieren](#)
- [\[SageMaker.6\] SageMaker App-Image-Konfigurationen sollten mit Tags versehen werden](#)
- [\[SageMaker.7\] SageMaker Bilder sollten mit Tags versehen werden](#)
- [\[SNS.4\] Zugriffsrichtlinien für SNS-Themen sollten keinen öffentlichen Zugriff zulassen](#)
- [\[SQS.3\] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen](#)
- [\[SSM.4\] SSM-Dokumente sollten nicht öffentlich sein](#)
- [\[SSM.5\] SSM-Dokumente sollten mit Tags versehen werden](#)
- [\[StepFunctions.1\] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben](#)

- [\[StepFunctions.2\] Die Aktivitäten von Step Functions sollten mit Tags versehen werden](#)
- [\[Transfer.4\] Transfer Family Familienverträge sollten gekennzeichnet werden](#)
- [\[Transfer.5\] Transfer Family Familienzertifikate sollten gekennzeichnet sein](#)
- [\[Transfer.6\] Steckverbinder der Transfer-Familie sollten gekennzeichnet sein](#)
- [\[Transfer.7\] Familienprofile sollten mit Tags versehen werden](#)
- [\[WAF.1\] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein](#)
- [\[WAF.2\] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.3\] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.4\] AWS WAF Classic Regional Web ACLs sollte mindestens eine Regel oder Regelgruppe enthalten](#)
- [\[WAF.6\] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben](#)
- [\[WAF.7\] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben](#)
- [\[WAF.8\] Das AWS WAF klassische globale Web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [\[WAF.10\] AWS WAF web ACLs sollte mindestens eine Regel oder Regelgruppe haben](#)
- [Für \[WAF.12\] AWS WAF Regeln sollten Metriken aktiviert sein CloudWatch](#)

Security Hub CSPM-Ressourcen erstellen mit CloudFormation

AWS Security Hub Cloud Security Posture Management (CSPM) lässt sich in diesen Service integrieren AWS CloudFormation, der Sie bei der Modellierung und Einrichtung Ihrer AWS Ressourcen unterstützt, sodass Sie weniger Zeit mit der Erstellung und Verwaltung Ihrer Ressourcen und Infrastruktur verbringen müssen. Sie erstellen eine Vorlage, die alle gewünschten AWS Ressourcen beschreibt (z. B. Automatisierungsregeln) und diese Ressourcen für Sie AWS CloudFormation bereitstellt und konfiguriert.

Wenn Sie sie verwenden AWS CloudFormation, können Sie Ihre Vorlage wiederverwenden, um Ihre Security Hub CSPM-Ressourcen konsistent und wiederholt einzurichten. Beschreiben Sie Ihre Ressourcen einmal und stellen Sie dann dieselben Ressourcen immer wieder in mehreren Regionen bereit AWS-Konten .

Security Hub CSPM und Vorlagen AWS CloudFormation

Um Ressourcen für Security Hub CSPM und verwandte Dienste bereitzustellen und zu konfigurieren, müssen Sie wissen, wie [AWS CloudFormation Vorlagen](#) funktionieren. Vorlagen sind Textdateien im JSON- oder YAML-Format. Diese Vorlagen beschreiben die Ressourcen, die Sie in Ihren AWS CloudFormation Stacks bereitstellen möchten.

Wenn Sie mit JSON oder YAML nicht vertraut sind, können Sie AWS CloudFormation Designer verwenden, um Ihnen die ersten Schritte mit Vorlagen zu erleichtern. AWS CloudFormation Weitere Informationen finden Sie unter [Was ist AWS CloudFormation Designer?](#) im AWS CloudFormation Benutzerhandbuch.

Sie können AWS CloudFormation Vorlagen für die folgenden Typen von Security Hub CSPM-Ressourcen erstellen:

- Security Hub CSPM aktivieren
- Benennen des delegierten Security Hub CSPM-Administrators für eine Organisation
- Geben Sie an, wie Ihre Organisation in Security Hub CSPM konfiguriert ist
- Aktivierung eines Sicherheitsstandards
- Aktivierung der regionsübergreifenden Aggregation

- Eine zentrale Konfigurationsrichtlinie erstellen und sie Konten, Organisationseinheit (OUs) oder dem Stamm zuordnen
- Einen benutzerdefinierten Einblick erstellen
- Eine Automatisierungsregel erstellen
- Anpassen von Steuerungsparametern
- Abonnieren Sie eine Produktintegration eines Drittanbieters

Weitere Informationen, einschließlich Beispielen für JSON- und YAML-Vorlagen für Ressourcen, finden Sie in der [Referenz zum Ressourcentyp AWS Security Hub Cloud Security Posture Management \(CSPM\) im AWS CloudFormation Benutzerhandbuch](#).

Erfahren Sie mehr über AWS CloudFormation

Weitere Informationen AWS CloudFormation dazu finden Sie in den folgenden Ressourcen:

- [AWS CloudFormation](#)
- [AWS CloudFormation Benutzerhandbuch](#)
- [AWS CloudFormation API Reference](#)
- [AWS CloudFormation Benutzerhandbuch für die Befehlszeilenschnittstelle](#)

Abonnieren von Security Hub CSPM-Ankündigungen mit Amazon SNS

Dieser Abschnitt enthält Informationen zum Abonnieren von Ankündigungen von AWS Security Hub Cloud Security Posture Management (CSPM) mit Amazon Simple Notification Service (Amazon SNS), um Benachrichtigungen über Security Hub CSPM zu erhalten.

Nach dem Abonnieren erhalten Sie Benachrichtigungen über die folgenden Ereignisse (beachten Sie die entsprechenden Ereignisse): `AnnouncementType`

- `GENERAL`— Allgemeine Benachrichtigungen über den Security Hub CSPM-Dienst.
- `UPCOMING_STANDARDS_CONTROLS`— Spezifizierte Security Hub CSPM-Steuerungen oder -Standards werden in Kürze veröffentlicht. Diese Art der Ankündigung hilft Ihnen dabei, Reaktions- und Behebungsabläufe im Vorfeld einer Veröffentlichung vorzubereiten.
- `NEW_REGIONS`— Die Support für Security Hub CSPM ist in einer neuen Version verfügbar. AWS-Region
- `NEW_STANDARDS_CONTROLS`— Neue Security Hub CSPM-Steuerungen oder -Standards wurden hinzugefügt.
- `UPDATED_STANDARDS_CONTROLS`— Bestehende Security Hub CSPM-Kontrollen oder -Standards wurden aktualisiert.
- `RETIRED_STANDARDS_CONTROLS`— Bestehende Security Hub CSPM-Kontrollen oder -Standards wurden eingestellt.
- `UPDATED_ASFF`— Die Syntax, Felder oder Werte des AWS Security Finding Format (ASFF) wurden aktualisiert.
- `NEW_INTEGRATION`— Neue Integrationen mit anderen AWS Diensten oder Produkten von Drittanbietern sind verfügbar.
- `NEW_FEATURE`— Neue Security Hub CSPM-Funktionen sind verfügbar.
- `UPDATED_FEATURE`— Bestehende Security Hub CSPM-Funktionen wurden aktualisiert.

Benachrichtigungen sind in allen Formaten verfügbar, die Amazon SNS unterstützt. Sie können die Ankündigungen von Security Hub CSPM in allen Bereichen abonnieren, in [AWS-Regionen denen Security Hub CSPM verfügbar](#) ist.

Ein Benutzer muss über `Subscribe` Berechtigungen verfügen, um ein Amazon SNS SNS-Thema zu abonnieren. Sie können dies mit Amazon SNS SNS-Richtlinien, IAM-Richtlinien oder beidem erreichen. Weitere Informationen finden Sie unter [IAM- und Amazon SNS SNS-Richtlinien zusammen](#) im Amazon Simple Notification Service Developer Guide.

 Note

Security Hub CSPM sendet Amazon SNS SNS-Ankündigungen über Updates für den Security Hub CSPM-Service an alle Abonnenten. AWS-Konto Informationen zum Erhalt von Benachrichtigungen über die Ergebnisse von Security Hub CSPM finden Sie unter [Überprüfung der Funddetails und des Verlaufs in Security Hub CSPM](#)

Sie können eine Amazon Simple Queue Service (Amazon SQS) -Warteschlange für ein Amazon SNS SNS-Thema abonnieren, müssen jedoch einen Amazon SNS SNS-Thema Amazon Resource Name (ARN) verwenden, der sich in derselben Region befindet. Weitere Informationen finden Sie unter [Abonnieren einer Warteschlange für ein Amazon SNS](#) im Amazon Simple Queue Service Developer Guide.

Sie können auch eine AWS Lambda Funktion verwenden, um Ereignisse auszulösen, wenn Sie Benachrichtigungen erhalten. Weitere Informationen, einschließlich Beispielfunktionscode, finden Sie unter [Tutorial: Using AWS Lambda with Amazon Simple Notification Service](#) im AWS Lambda Entwicklerhandbuch.

Die Amazon SNS-Themen ARNs für jede Region lauten wie folgt.

AWS-Region	ARN des Amazon-SNS-Themas
US East (Ohio)	<code>arn:aws:sns:us-east-2:291342846459:SecurityHubAnnouncements</code>
USA Ost (Nord-Virginia)	<code>arn:aws:sns:us-east-1:088139225913:SecurityHubAnnouncements</code>

AWS-Region	ARN des Amazon-SNS-Themas
USA West (Nordkalifornien)	arn:aws:sns:us-west-1:137690824926:SecurityHubAnnouncements
USA West (Oregon)	arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements
Africa (Cape Town)	arn:aws:sns:af-south-1:463142546776:SecurityHubAnnouncements
Asien-Pazifik (Hongkong)	arn:aws:sns:ap-east-1:464812404305:SecurityHubAnnouncements
Asien-Pazifik (Hyderabad)	arn:aws:sns:ap-south-2:849907286123:SecurityHubAnnouncements
Asien-Pazifik (Jakarta)	arn:aws:sns:ap-southeast-3:627843640627:SecurityHubAnnouncements
Asien-Pazifik (Mumbai)	arn:aws:sns:ap-south-1:707356269775:SecurityHubAnnouncements
Asien-Pazifik (Osaka)	arn:aws:sns:ap-northeast-3:633550238216:SecurityHubAnnouncements
Asien-Pazifik (Seoul)	arn:aws:sns:ap-northeast-2:374299265323:SecurityHubAnnouncements

AWS-Region	ARN des Amazon-SNS-Themas
Asien-Pazifik (Singapur)	<code>arn:aws:sns:ap-southeast-1:512267288502:SecurityHubAnnouncements</code>
Asien-Pazifik (Sydney)	<code>arn:aws:sns:ap-southeast-2:475730049140:SecurityHubAnnouncements</code>
Asien-Pazifik (Tokio)	<code>arn:aws:sns:ap-northeast-1:592469075483:SecurityHubAnnouncements</code>
Canada (Central)	<code>arn:aws:sns:ca-central-1:137749997395:SecurityHubAnnouncements</code>
China (Peking)	<code>arn:aws-cn:sns:cn-north-1:672341567257:SecurityHubAnnouncements</code>
China (Ningxia)	<code>arn:aws-cn:sns:cn-northwest-1:672534482217:SecurityHubAnnouncements</code>
Europe (Frankfurt)	<code>arn:aws:sns:eu-central-1:871975303681:SecurityHubAnnouncements</code>
Europa (Irland)	<code>arn:aws:sns:eu-west-1:705756202095:SecurityHubAnnouncements</code>
Europa (London)	<code>arn:aws:sns:eu-west-2:883600840440:SecurityHubAnnouncements</code>

AWS-Region	ARN des Amazon-SNS-Themas
Europa (Milan)	arn:aws:sns:eu-south-1:151363035580:SecurityHubAnnouncements
Europa (Paris)	arn:aws:sns:eu-west-3:313420042571:SecurityHubAnnouncements
Europa (Spain)	arn:aws:sns:eu-south-2:777487947751:SecurityHubAnnouncements
Europa (Stockholm)	arn:aws:sns:eu-north-1:191971010772:SecurityHubAnnouncements
Europa (Zürich)	arn:aws:sns:eu-central-2:704347005078:SecurityHubAnnouncements
Israel (Tel Aviv)	arn:aws:sns:il-central-1:726652212146:SecurityHubAnnouncements
Naher Osten (Bahrain)	arn:aws:sns:me-south-1:585146626860:SecurityHubAnnouncements
Naher Osten (VAE)	arn:aws:sns:me-central-1:431548502100:SecurityHubAnnouncements
Südamerika (São Paulo)	arn:aws:sns:sa-east-1:359811883282:SecurityHubAnnouncements

AWS-Region	ARN des Amazon-SNS-Themas
AWS GovCloud (USA-Ost)	arn:aws-us-gov:sns:us-gov-east-1:239368469855:SecurityHubAnnouncements
AWS GovCloud (US-West)	arn:aws-us-gov:sns:us-gov-west-1:239334163374:SecurityHubAnnouncements

Nachrichten sind in der Regel in allen Regionen innerhalb einer [Partition](#) identisch. Sie können also eine Region in jeder Partition abonnieren, um Ankündigungen zu erhalten, die sich auf alle Regionen in dieser Partition auswirken. Ankündigungen, die mit Mitgliedskonten verknüpft sind, werden nicht im Administratorkonto repliziert. Daher verfügt jedes Konto, einschließlich des Administratorkontos, nur über eine Kopie jeder Ankündigung. Sie können entscheiden, welches Konto Sie verwenden möchten, um Security Hub CSPM-Ankündigungen zu abonnieren.

Informationen zu den Kosten für das Abonnieren von Security Hub CSPM-Ankündigungen finden Sie unter [Amazon SNS SNS-Preise](#).

Security Hub CSPM-Ankündigungen abonnieren (Konsole)

1. Öffnen Sie die Amazon SNS SNS-Konsole unter <https://console.aws.amazon.com/sns/v3/home>.
2. Wählen Sie in der Liste Region die Region aus, in der Sie Security Hub CSPM-Ankündigungen abonnieren möchten. In diesem Beispiel wird die Region us-west-2 verwendet.
3. Wählen Sie im Navigationsbereich Subscriptions (Abonnements) und dann Create subscription (Abonnement erstellen) aus.
4. Geben Sie den Themen-ARN in das Feld Themen-ARN ein. Beispiel, arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements.
5. Wählen Sie unter Protokoll aus, wie Sie Security Hub CSPM-Ankündigungen erhalten möchten. Wenn Sie E-Mail wählen, geben Sie für Endpoint die E-Mail-Adresse ein, die Sie für den Empfang von Ankündigungen verwenden möchten.
6. Wählen Sie Create subscription (Abonnement erstellen) aus.
7. Bestätigen Sie das Abonnement. Wenn Sie beispielsweise das E-Mail-Protokoll ausgewählt haben, sendet Amazon SNS eine Bestätigungsnachricht für das Abonnement an die von Ihnen angegebene E-Mail-Adresse.

Abonnieren von Security Hub CSPM-Ankündigungen (AWS CLI)

1. Führen Sie den folgenden Befehl aus:

```
aws sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements --protocol email --notification-endpoint your_email@your_domain.com
```

2. Bestätigen Sie das Abonnement. Wenn Sie beispielsweise das E-Mail-Protokoll ausgewählt haben, sendet Amazon SNS eine Bestätigungsnachricht für das Abonnement an die von Ihnen angegebene E-Mail-Adresse.

Amazon-SNS-Nachrichtenformat

Die folgenden Beispiele zeigen Security Hub CSPM-Ankündigungen von Amazon SNS zur Einführung neuer Sicherheitskontrollen. Der Nachrichteninhalt variiert je nach Art der Ankündigung, aber das Format ist für alle Ankündigungstypen gleich. Optional kann ein Link Feld mit Details zur Ankündigung hinzugefügt werden.

Beispiel: Security Hub CSPM-Ankündigung für neue Kontrollen (E-Mail-Protokoll)

```
{
  "AnnouncementType": "NEW_STANDARDS_CONTROLS",
  "Title": "[New Controls] 36 new Security Hub CSPM controls added to the AWS Foundational Security Best Practices standard",
  "Description": "We have added 36 new controls to the AWS Foundational Security Best Practices standard. These include controls for Amazon Auto Scaling (AutoScaling.3, AutoScaling.4, AutoScaling.6), AWS CloudFormation (CloudFormation.1), Amazon CloudFront (CloudFront.10), Amazon Elastic Compute Cloud (Amazon EC2) (EC2.23, EC2.24, EC2.27), Amazon Elastic Container Registry (Amazon ECR) (ECR.1, ECR.2), Amazon Elastic Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5, ECS.8, ECS.10, ECS.12), Amazon Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon Elastic Kubernetes Service (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12, ELB.13, ELB.14), Amazon Kinesis (Kinesis.1), AWS Network Firewall (NetworkFirewall.3, NetworkFirewall.4, NetworkFirewall.5), Amazon OpenSearch Service (OpenSearch.7), Amazon Redshift (Redshift.9), Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification Service (SNS.2), AWS WAF (WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled the AWS Foundational Security Best Practices standard in an account and configured Security Hub CSPM to automatically enable new controls, these controls are enabled by default. Availability of controls can vary by Region. "
```


}

Beispiel: Security Hub CSPM-Ankündigung für neue Kontrollen (E-Mail-JSON-Protokoll)

```
{
  "Type" : "Notification",
  "MessageId" : "d124c9cf-326a-5931-9263-92a92e7af49f",
  "TopicArn" : "arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements",
  "Message" : "{\"AnnouncementType\":\"NEW_STANDARDS_CONTROLS\",\"Title\":\"[New Controls] 36 new Security Hub CSPM controls added to the AWS Foundational Security Best Practices standard\",\"Description\":\"We have added 36 new controls to the AWS Foundational Security Best Practices standard. These include controls for Amazon Auto Scaling (AutoScaling.3, AutoScaling.4, AutoScaling.6), AWS CloudFormation (CloudFormation.1), Amazon CloudFront (CloudFront.10), Amazon Elastic Compute Cloud (Amazon EC2) (EC2.23, EC2.24, EC2.27), Amazon Elastic Container Registry (Amazon ECR) (ECR.1, ECR.2), Amazon Elastic Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5, ECS.8, ECS.10, ECS.12), Amazon Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon Elastic Kubernetes Service (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12, ELB.13, ELB.14), Amazon Kinesis (Kinesis.1), AWS Network Firewall (NetworkFirewall.3, NetworkFirewall.4, NetworkFirewall.5), Amazon OpenSearch Service (OpenSearch.7), Amazon Redshift (Redshift.9), Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification Service (SNS.2), AWS WAF (WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled the AWS Foundational Security Best Practices standard in an account and configured SSecurity Hub CSPM to automatically enable new controls, these controls are enabled by default. Availability of controls can vary by Region. \"}",
  "Timestamp" : "2022-08-04T19:11:12.652Z",
  "SignatureVersion" : "1",
  "Signature" :
    "HTHgNFRYMetCvisulgLm4CVySvK9qCXFPHQDxYl9tuCFQuIrd7Y04m4YFR28XKMgzqrF20YP
    +EilipUm2S0TpEEt0TekU5bn74+YmNZfwr4aPFx0vUuQCV0shmHl37hjkilJhCg/t53QQiLfp7MH
    +MTXIUPR37k5SuFCXvjpRQ8ynV532AH3Wpv0HmojDLMg+eg51V1fUs0G8yiJVCBEJhJ1yS
    +gkwJdhRk2UQab9RcAmE6COK3hRwcjDwqTXz5nR6Ywv1ZqZfLi17gYKslt+jsyd/k+7k0qGm0JRD7qhE7H
    +7vaGRL0ptsQnbW8VmeYnDbahE08FV+Mp1rpV+7Qg==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
  SimpleNotificationService-56e67fcb41f6fec09b0196692625d385.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
  Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
  west-2:393883065485:SecurityHubAnnouncements:9d0230d7-d582-451d-9f15-0c32818bf61f"
}
```

Security Hub CSPM deaktivieren

Sie können AWS Security Hub Cloud Security Posture Management (CSPM) mithilfe der Security Hub CSPM-Konsole oder der Security Hub Hub-API deaktivieren. Wenn Sie Security Hub CSPM deaktivieren, können Sie es später wieder aktivieren.

Wenn Ihre Organisation die zentrale Konfiguration verwendet, kann der delegierte Security Hub CSPM-Administrator Konfigurationsrichtlinien erstellen, die Security Hub CSPM für bestimmte Konten und Organisationseinheiten deaktivieren (OUs) und Security Hub CSPM für andere aktivieren. Die Konfigurationsrichtlinien wirken sich auf die Heimatregion und alle verknüpften Regionen aus. Weitere Informationen finden Sie unter [Grundlegendes zur zentralen Konfiguration in Security Hub CSPM](#).

Wenn Sie Security Hub CSPM für ein Konto deaktivieren, passiert Folgendes:

- Alle Security Hub CSPM-Standards und -Kontrollen sind für das Konto deaktiviert.
- Security Hub CSPM beendet die Generierung, Aktualisierung und Erfassung von Ergebnissen für das Konto.
- Nach 30 Tagen löscht Security Hub CSPM dauerhaft alle vorhandenen archivierten Ergebnisse für das Konto. Die Ergebnisse können mit Security Hub CSPM nicht wiederhergestellt werden.
- Nach 90 Tagen löscht Security Hub CSPM dauerhaft alle vorhandenen aktiven Ergebnisse für das Konto. Die Ergebnisse können mit Security Hub CSPM nicht wiederhergestellt werden.
- Nach 90 Tagen löscht Security Hub CSPM dauerhaft alle vorhandenen Insights und Security Hub CSPM-Konfigurationseinstellungen für das Konto. Die Daten und Einstellungen können nicht wiederhergestellt werden.

Um bestehende Ergebnisse beizubehalten, können Sie die Ergebnisse in einen S3-Bucket exportieren, bevor Sie Security Hub CSPM deaktivieren. Sie können dies tun, indem Sie eine benutzerdefinierte Aktion mit einer EventBridge Amazon-Regel verwenden. Weitere Informationen finden Sie unter [Verwendung EventBridge für automatisierte Reaktionen und Problembehebungen](#).

Wenn Sie Security Hub CSPM innerhalb von 90 Tagen nach der Deaktivierung für ein Konto erneut aktivieren, erhalten Sie wieder Zugriff auf bestehende aktive Ergebnisse sowie auf Einblicke und Security Hub CSPM-Konfigurationseinstellungen für das Konto. Wenn Sie Security Hub CSPM innerhalb von 30 Tagen erneut aktivieren, erhalten Sie auch wieder Zugriff auf bestehende archivierte Ergebnisse für das Konto. Bestehende Ergebnisse können jedoch ungenau sein, da sie den Zustand

Ihrer AWS Umgebung widerspiegeln, als Sie Security Hub CSPM deaktiviert haben. Wenn Sie einzelne Standards und Kontrollen wieder aktivieren, generiert Security Hub CSPM außerdem möglicherweise zunächst doppelte Ergebnisse für bestimmte AWS Ressourcen, je nachdem, welche Standards und Kontrollen Sie aktivieren. Aus diesen Gründen empfehlen wir Ihnen, einen der folgenden Schritte durchzuführen:

- Ändern Sie den Workflow-Status aller vorhandenen Ergebnisse auf „RESOLVED“. Bevor Sie Security Hub CSPM deaktivieren. Weitere Informationen finden Sie unter [Den Workflow-Status von Ergebnissen festlegen](#).
- Deaktivieren Sie alle Standards mindestens sechs Tage vor der Deaktivierung von Security Hub CSPM. Security Hub CSPM archiviert dann alle vorhandenen Ergebnisse nach bestem Wissen und Gewissen, in der Regel innerhalb von drei bis fünf Tagen. Weitere Informationen finden Sie unter [Deaktivierung eines Standards](#).

In den folgenden Fällen können Sie Security Hub CSPM nicht deaktivieren:

- Ihr Konto ist das delegierte Security Hub CSPM-Administratorkonto für eine Organisation. Wenn Sie die zentrale Konfiguration verwenden, können Sie keine Konfigurationsrichtlinie zuordnen, die Security Hub CSPM für das delegierte Administratorkonto deaktiviert. Die Zuordnung kann für andere Konten erfolgreich sein, aber Security Hub CSPM wendet die Richtlinie nicht auf das delegierte Administratorkonto an.
- Ihr Konto ist auf Einladung ein Security Hub CSPM-Administratorkonto, und Sie haben Mitgliedskonten. Bevor Sie Security Hub CSPM deaktivieren können, müssen Sie alle Ihre Mitgliedskonten trennen. Um zu erfahren wie dies geht, vgl. [the section called “Aufheben der Zuordnung von Mitgliedskonten”](#).

Bevor der Besitzer eines Mitgliedskontos Security Hub CSPM deaktivieren kann, muss das Konto von seinem Administratorkonto getrennt werden. Bei einem Organisationskonto kann nur das Administratorkonto die Zuordnung zu einem Mitgliedskonto aufheben. Weitere Informationen finden Sie unter [the section called “Aufheben der Zuordnung von Mitgliedskonten der Organisation”](#). Bei einem manuell eingeladenen Konto kann entweder das Administratorkonto oder das Mitgliedskonto die Zuordnung des Kontos aufheben. Weitere Informationen finden Sie unter [the section called “Aufheben der Zuordnung von Mitgliedskonten”](#) oder [the section called “Trennung von einem Administratorkonto”](#). Eine Trennung ist nicht erforderlich, wenn Sie die zentrale Konfiguration verwenden, da der Security Hub CSPM-Administrator eine Richtlinie erstellen kann, die Security Hub CSPM für bestimmte Mitgliedskonten deaktiviert.

Wenn Sie Security Hub CSPM für ein Konto deaktivieren, ist es nur aktuell deaktiviert. AWS-Region
Wenn Sie jedoch die zentrale Konfiguration verwenden, um Security Hub CSPM für bestimmte
Konten zu deaktivieren, ist es in der Heimatregion und allen verknüpften Regionen deaktiviert.

Um Security Hub CSPM zu deaktivieren, wählen Sie Ihre bevorzugte Methode und folgen Sie den
Schritten.

Security Hub CSPM console

Gehen Sie wie folgt vor, um Security Hub CSPM mithilfe der Konsole zu deaktivieren.

So deaktivieren Sie Security Hub CSPM

1. Öffnen Sie die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>
2. Klicken Sie im Navigationsbereich unter Settings auf General.
3. Wählen Sie im Abschnitt Security Hub CSPM deaktivieren die Option Security Hub CSPM deaktivieren.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Disable Security Hub CSPM.

Security Hub API

Verwenden Sie den [DisableSecurityHub](#) Betrieb der Security Hub-API, um Security Hub CSPM
programmgesteuert zu deaktivieren. AWS Oder, wenn Sie den verwenden, führen Sie den Befehl
aus AWS CLI. [disable-security-hub](#) Beispielsweise deaktiviert der folgende Befehl Security Hub
CSPM in der aktuellen Version: AWS-Region

```
$ aws securityhub disable-security-hub
```

Sicherheit in AWS Security Hub

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das [Modell der geteilten Verantwortung](#) beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- **Sicherheit der Cloud** — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der [AWS -Compliance-Programme](#) regelmäßig. Weitere Informationen zu den Compliance-Programmen für AWS Security Hub finden Sie unter [Durch das Compliance-Programm abgedeckte AWS -Services](#).
- **Sicherheit in der Cloud** — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von Security Hub anwenden können. In den folgenden Themen erfahren Sie, wie Sie Security Hub so konfigurieren, dass Sie Ihre Sicherheits- und Compliance-Ziele erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, mit denen Sie Ihre Security Hub Hub-Ressourcen überwachen und sichern können.

Themen

- [Datenschutz in AWS Security Hub](#)
- [AWS Identity and Access Management für Security Hub](#)
- [Compliance-Validierung für AWS Security Hub](#)
- [Resilienz im AWS Security Hub](#)
- [Infrastruktursicherheit in AWS Security Hub](#)
- [AWS Security Hub und Schnittstellen-VPC-Endpunkte \(\)AWS PrivateLink](#)

Datenschutz in AWS Security Hub

Das AWS [Modell](#) der gilt für den Datenschutz in AWS Security Hub. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter [Häufig gestellte Fragen zum Datenschutz](#). Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag [AWS -Modell der geteilten Verantwortung und in der DSGVO](#) im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter [Arbeiten mit CloudTrail Pfaden](#) im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter [Federal Information Processing Standard \(FIPS\) 140-3](#).

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dazu gehört auch, wenn Sie mit Security Hub oder anderen AWS-Services über die Konsole AWS CLI, API oder arbeiten AWS SDKs. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen

Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Security Hub ist ein Serviceangebot für mehrere Mandanten. Um den Datenschutz zu gewährleisten, verschlüsselt Security Hub ruhende Daten und Daten, die zwischen Komponentendiensten übertragen werden.

AWS Identity and Access Management für Security Hub

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service, den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Security Hub Hub-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service, das Sie ohne zusätzliche Kosten nutzen können.

Themen

- [Zielgruppe](#)
- [Authentifizierung mit Identitäten](#)
- [Verwalten des Zugriffs mit Richtlinien](#)
- [So funktioniert Security Hub mit IAM](#)
- [Beispiele für identitätsbasierte Richtlinien für AWS Security Hub](#)
- [Mit Diensten verknüpfte Rollen für AWS Security Hub](#)
- [AWS verwaltete Richtlinien für Security Hub](#)
- [Fehlerbehebung bei AWS Security Hub Identität und Zugriff](#)

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in Security Hub ausführen.

Dienstbenutzer — Wenn Sie den Security Hub Hub-Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen zur Verfügung, die Sie benötigen. Da Sie für Ihre Arbeit mehr Security Hub Hub-Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Wenn

Sie auf eine Funktion in Security Hub nicht zugreifen können, finden Sie weitere Informationen unter [Fehlerbehebung bei AWS Security Hub Identität und Zugriff](#).

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die Security Hub-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf Security Hub. Es ist Ihre Aufgabe, zu bestimmen, auf welche Funktionen und Ressourcen von Security Hub Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anforderungen an Ihren IAM-Administrator senden, um die Berechtigungen der Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit Security Hub verwenden kann, finden Sie unter [So funktioniert Security Hub mit IAM](#).

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf Security Hub zu verwalten. Beispiele für identitätsbasierte Security Hub Richtlinien, die Sie in IAM verwenden können, finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Security Hub](#)

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter [So melden Sie sich bei Ihrem an AWS-Konto](#) im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode für die Selbstsignierung

von Anforderungen finden Sie unter [AWS Signature Version 4 für API-Anforderungen](#) im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen bereitstellen. AWS empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter [Multi-Faktor-Authentifizierung](#) im AWS IAM Identity Center - Benutzerhandbuch und [AWS Multi-Faktor-Authentifizierung \(MFA\) in IAM](#) im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie ein AWS-Konto erstellen, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen. Verwenden Sie diese nur, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter [Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern](#) im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter [Was ist IAM Identity Center?](#) im AWS IAM Identity Center - Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein [IAM-Benutzer](#) ist eine Identität innerhalb Ihres Unternehmens AWS-Konto, die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter [Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern](#) im IAM-Benutzerhandbuch.

Eine [IAM-Gruppe](#) ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise eine Gruppe benennen IAMAdmins und dieser Gruppe Berechtigungen zur Verwaltung von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter [Anwendungsfälle für IAM-Benutzer](#) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine [IAM-Rolle](#) ist eine Identität innerhalb von Ihrem AWS-Konto, die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, jedoch nicht mit einer bestimmten Person verknüpft. Um vorübergehend eine IAM-Rolle in der zu übernehmen AWS Management Console, können Sie [von einer Benutzer- zu einer IAM-Rolle \(Konsole\) wechseln](#). Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter [Methoden für die Übernahme einer Rolle](#) im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter [Erstellen von Rollen für externe](#)

[Identitätsanbieter \(Verbund\)](#) im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter [Berechtigungssätze](#) im AWS IAM Identity Center -Benutzerhandbuch.

- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [Kontoübergreifender Ressourcenzugriff in IAM](#) im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise in einem Service einen Anruf tätigen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
- Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).
- Servicerolle – Eine Servicerolle ist eine [IAM-Rolle](#), die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter [Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service](#) im IAM-Benutzerhandbuch.
- Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und

gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

- Auf Amazon ausgeführte Anwendungen EC2 — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API-Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter [Verwenden einer IAM-Rolle, um Berechtigungen für Anwendungen zu gewähren, die auf EC2 Amazon-Instances ausgeführt werden](#).

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Die Berechtigungen in den Richtlinien legen fest, ob eine Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter [Übersicht über JSON-Richtlinien](#) im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter [Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien](#) im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer Inline-Richtlinie wählen, finden Sie unter [Auswählen zwischen verwalteten und eingebundenen Richtlinien](#) im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie [einen Prinzipal angeben](#). Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Dienste, die Unterstützung ACLs bieten. AWS WAF
Weitere Informationen finden Sie unter [Übersicht über ACLs die Zugriffskontrollliste \(ACL\)](#) im Amazon Simple Storage Service Developer Guide.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- **Berechtigungsgrenzen** – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter [Berechtigungsgrenzen für IAM-Entitäten](#) im IAM-Benutzerhandbuch.
- **Dienststeuerungsrichtlinien (SCPs)** — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos Entitäten. Weitere Informationen zu Organizations und SCPs finden Sie unter [Richtlinien zur Servicesteuerung](#) im AWS Organizations Benutzerhandbuch.
- **Ressourcenkontrollrichtlinien (RCPs)** — RCPs sind JSON-Richtlinien, mit denen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten festlegen können, ohne die IAM-Richtlinien aktualisieren zu müssen, die jeder Ressource zugeordnet sind, deren Eigentümer Sie sind. Das RCP schränkt die Berechtigungen für Ressourcen in Mitgliedskonten ein und kann sich auf die effektiven Berechtigungen für Identitäten auswirken, einschließlich der Root-Benutzer des AWS-Kontos, unabhängig davon, ob sie zu Ihrer Organisation gehören. Weitere Informationen zu Organizations RCPs, einschließlich einer Liste AWS-Services dieser Support-Leistungen RCPs, finden Sie unter [Resource Control Policies \(RCPs\)](#) im AWS Organizations Benutzerhandbuch.

- **Sitzungsrichtlinien** – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter [Sitzungsrichtlinien](#) im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter [Bewertungslogik für Richtlinien](#).

So funktioniert Security Hub mit IAM

Bevor Sie AWS Identity and Access Management (IAM) zur Verwaltung des Zugriffs auf verwenden AWS Security Hub, sollten Sie sich darüber informieren, welche IAM-Funktionen mit Security Hub verwendet werden können.

IAM-Funktionen, die Sie mit verwenden können AWS Security Hub

IAM-Feature	Security Hub Hub-Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Nein
Bedingungsschlüssel für die Richtlinie	Ja
Zugriffskontrolllisten (ACLs)	Nein
Attributbasierte Zugriffskontrolle (ABAC) — Tags in Richtlinien	Ja

IAM-Feature	Security Hub Hub-Unterstützung
Temporäre Anmeldeinformationen	Ja
Forward Access Sessions (FAS)	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie Security Hub und andere mit den meisten IAM-Funktionen AWS-Services funktionieren [AWS-Services](#) , finden Sie im [IAM-Benutzerhandbuch unter Diese funktionieren mit IAM](#).

Identitätsbasierte Richtlinien für Security Hub

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter [Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien](#) im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der [IAM-Referenz für JSON-Richtlinienelemente](#) im IAM-Benutzerhandbuch.

Security Hub unterstützt identitätsbasierte Richtlinien. Weitere Informationen finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Security Hub](#).

Ressourcenbasierte Richtlinien für Security Hub

Unterstützt ressourcenbasierte Richtlinien: Nein

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie [einen Prinzipal angeben](#). Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos auch der Prinzipalentsität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter [Kontoübergreifender Ressourcenzugriff in IAM](#) im IAM-Benutzerhandbuch.

Security Hub unterstützt keine ressourcenbasierten Richtlinien. Sie können eine IAM-Richtlinie nicht direkt an eine Security Hub Hub-Ressource anhängen.

Richtlinienaktionen für Security Hub

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Richtlinienaktionen in Security Hub verwenden vor der Aktion das folgende Präfix:

```
securityhub:
```

Um einem Benutzer beispielsweise die Erlaubnis zu erteilen, Security Hub zu aktivieren, was eine Aktion ist, die dem EnableSecurityHub Betrieb der Security Hub Hub-API entspricht, nehmen Sie die securityhub:EnableSecurityHub Aktion in seine Richtlinie auf. Richtlinienanweisungen müssen entweder ein – Actionoder ein NotAction-Element enthalten. Security Hub definiert eigene Aktionen, die Aufgaben beschreiben, die Sie mit diesem Dienst ausführen können.

```
"Action": "securityhub:EnableSecurityHub"
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata: Zum Beispiel:

```
"Action": [  
    "securityhub:EnableSecurityHub",  
    "securityhub:BatchEnableStandards"
```

Sie können auch mehrere Aktionen mithilfe von Platzhaltern (*) angeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort Get beginnen, einschließlich der folgenden Aktion:

```
"Action": "securityhub:Get*"
```

Als bewährte Methode sollten Sie jedoch Richtlinien erstellen, die dem Prinzip der geringsten Rechte folgen. Mit anderen Worten, Sie sollten Richtlinien erstellen, die nur die Berechtigungen enthalten, die zum Ausführen einer bestimmten Aufgabe erforderlich sind.

Der Benutzer muss Zugriff auf den DescribeStandardsControl Vorgang haben, um auf BatchGetSecurityControlsBatchGetStandardsControlAssociations, und ListStandardsControlAssociations zugreifen zu können.

Der Benutzer muss Zugriff auf den UpdateStandardsControls Vorgang haben, um Zugriff aufBatchUpdateStandardsControlAssociations, und zu habenUpdateSecurityControl.

Eine Liste der Security Hub Hub-Aktionen finden Sie unter [Actions defined by AWS Security Hub](#) in der Service Authorization Reference. Beispiele für Richtlinien, die Security Hub Hub-Aktionen spezifizieren, finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Security Hub](#).

Richtlinienressourcen für Security Hub

Unterstützt politische Ressourcen: Nein

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein `Resource` oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen [Amazon-Ressourcennamen \(ARN\)](#) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*" 
```

Security Hub definiert die folgenden Ressourcentypen:

- Hub (Hub)
- Produkt
- Finding-Aggregator, auch als regionsübergreifender Aggregator bezeichnet
- Automatisierungsregel
- Konfigurationsrichtlinie

Sie können diese Ressourcentypen in Richtlinien angeben, indem Sie ARNs

Eine Liste der Security Hub Hub-Ressourcentypen und der jeweiligen ARN-Syntax finden Sie unter [Ressourcentypen definiert von AWS Security Hub](#) in der Service Authorization Reference. Informationen darüber, welche Aktionen Sie für die einzelnen Ressourcentypen angeben können, finden Sie unter [Aktionen definiert von AWS Security Hub](#) in der Service Authorization Reference. Beispiele für Richtlinien, die Ressourcen spezifizieren, finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Security Hub](#).

Schlüssel für Richtlinienbedingungen für Security Hub

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition block`) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die [Bedingungsoperatoren](#) verwenden, z. B. `ist gleich` oder `kleiner als`, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen AND-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen OR Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter [IAM-Richtlinienelemente: Variablen und Tags](#) im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter [Kontextschlüssel für AWS globale Bedingungen](#) im IAM-Benutzerhandbuch.

Eine Liste der Security Hub Hub-Bedingungsschlüssel finden Sie unter [Bedingungsschlüssel für AWS Security Hub](#) in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter [Aktionen definiert von AWS Security Hub](#). Beispiele für Richtlinien, die Bedingungsschlüssel verwenden, finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Security Hub](#).

Zugriffskontrolllisten (ACLs) in Security Hub

Unterstützt ACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Security Hub unterstützt nicht ACLs, was bedeutet, dass Sie einer Security Hub Hub-Ressource keine ACL zuordnen können.

Attributbasierte Zugriffskontrolle (ABAC) mit Security Hub

Unterstützt ABAC (Tags in Richtlinien): Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In werden AWS diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungelement einer [Richtlinie Tag-Informationen](#) an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter [Definieren von Berechtigungen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe [Attributbasierte Zugriffskontrolle \(ABAC\)](#) verwenden im IAM-Benutzerhandbuch.

Sie können Tags an Security Hub Hub-Ressourcen anhängen. Sie können den Zugriff auf Ressourcen auch kontrollieren, indem Sie Tag-Informationen im Condition Element einer Richtlinie angeben.

Informationen zum Taggen von Security Hub Hub-Ressourcen finden Sie unter [Kennzeichnung von Security Hub CSPM-Ressourcen](#). Ein Beispiel für eine identitätsbasierte Richtlinie, die den Zugriff auf eine Ressource anhand von Tags steuert, finden Sie unter. [Beispiele für identitätsbasierte Richtlinien für AWS Security Hub](#)

Temporäre Anmeldeinformationen mit Security Hub verwenden

Unterstützt temporäre Anmeldeinformationen: Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services [funktionieren AWS-Services](#) , [finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM](#).

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter [Wechseln von einer Benutzerrolle zu einer IAM-Rolle \(Konsole\)](#) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter [Temporäre Sicherheitsanmeldeinformationen in IAM](#).

Sie können temporäre Anmeldeinformationen verwenden, um sich über einen Verbund anzumelden, eine IAM-Rolle anzunehmen oder eine kontenübergreifende Rolle anzunehmen. Sie erhalten temporäre Sicherheitsanmeldedaten, indem Sie AWS STS API-Operationen wie [AssumeRole](#) oder aufrufen [GetFederationToken](#).

Security Hub unterstützt die Verwendung temporärer Anmeldeinformationen.

Zugriffssitzungen für Security Hub weiterleiten

Unterstützt Forward Access Sessions (FAS): Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).

Beispielsweise sendet Security Hub FAS-Anfragen an Downstream, AWS-Services wenn Sie Security Hub in Organizations integrieren AWS Organizations und wenn Sie das delegierte Security Hub-Administratorkonto für eine Organisation festlegen.

Für andere Aufgaben verwendet Security Hub eine dienstbezogene Rolle, um Aktionen in Ihrem Namen auszuführen. Einzelheiten zu dieser Rolle finden Sie unter [Mit Diensten verknüpfte Rollen für AWS Security Hub](#).

Servicerollen für Security Hub

Security Hub übernimmt oder verwendet keine Servicerollen. Um Aktionen in Ihrem Namen durchzuführen, verwendet Security Hub eine dienstbezogene Rolle. Einzelheiten zu dieser Rolle finden Sie unter [Mit Diensten verknüpfte Rollen für AWS Security Hub](#).

Warning

Das Ändern der Berechtigungen für eine Servicerolle kann zu Betriebsproblemen bei Ihrer Nutzung von Security Hub führen. Bearbeiten Sie Servicerollen nur, wenn Security Hub Sie dazu anleitet.

Serviceverknüpfte Rollen für Security Hub

Unterstützt serviceverknüpfte Rollen: Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Security Hub verwendet eine dienstbezogene Rolle, um Aktionen in Ihrem Namen durchzuführen. Einzelheiten zu dieser Rolle finden Sie unter [Mit Diensten verknüpfte Rollen für AWS Security Hub](#).

Beispiele für identitätsbasierte Richtlinien für AWS Security Hub

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Security Hub Hub-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mit der AWS Management Console AWS CLI, oder AWS API ausführen. Ein Administrator muss IAM-Richtlinien erstellen, die Benutzern und Rollen

die Berechtigung zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die diese benötigen. Der Administrator muss diese Richtlinien anschließend den - Benutzern oder -Gruppen anfügen, die diese Berechtigungen benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter [Erstellen von Richtlinien auf der JSON-Registerkarte](#) im IAM-Benutzerhandbuch.

Themen

- [Bewährte Methoden für Richtlinien](#)
- [Die Security Hub Hub-Konsole verwenden](#)
- [Beispiel: Erteilen der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer](#)
- [Beispiel: Erlauben Sie Benutzern, eine Konfigurationsrichtlinie zu erstellen und zu verwalten](#)
- [Beispiel: Erlauben Sie Benutzern, Ergebnisse einzusehen](#)
- [Beispiel: Erlauben Sie Benutzern, Automatisierungsregeln zu erstellen und zu verwalten](#)

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Security Hub Hub-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren, verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter [AWS -verwaltete Richtlinien](#) oder [AWS -verwaltete Richtlinien für Auftrags-Funktionen](#) im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum

Anwenden von Berechtigungen finden Sie unter [Richtlinien und Berechtigungen in IAM](#) im IAM-Benutzerhandbuch.

- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter [IAM-JSON-Richtlinienelemente: Bedingung](#) im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter [Richtlinienvvalidierung mit IAM Access Analyzer](#) im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter [Sicherer API-Zugriff mit MFA](#) im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter [Bewährte Methoden für die Sicherheit in IAM](#) im IAM-Benutzerhandbuch.

Die Security Hub Hub-Konsole verwenden

Um auf die AWS Security Hub Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Security Hub Hub-Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass diese Benutzer und Rollen die Security Hub Hub-Konsole verwenden können, fügen Sie der Entität auch die folgende AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter [Hinzufügen von Berechtigungen zu einem Benutzer](#) im IAM-Benutzerhandbuch:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "securityhub:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "iam:AWSServiceName": "securityhub.amazonaws.com"
        }
      }
    }
  ]
}
```

Beispiel: Erteilen der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie beinhaltet Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API AWS CLI oder AWS .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```

        "Sid": "ViewOwnUserInfo",
        "Effect": "Allow",
        "Action": [
            "iam:GetUserPolicy",
            "iam:ListGroupsForUser",
            "iam:ListAttachedUserPolicies",
            "iam:ListUserPolicies",
            "iam:GetUser"
        ],
        "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
        "Sid": "NavigateInConsole",
        "Effect": "Allow",
        "Action": [
            "iam:GetGroupPolicy",
            "iam:GetPolicyVersion",
            "iam:GetPolicy",
            "iam:ListAttachedGroupPolicies",
            "iam:ListGroupPolicies",
            "iam:ListPolicyVersions",
            "iam:ListPolicies",
            "iam:ListUsers"
        ],
        "Resource": "*"
    }
]
}

```

Beispiel: Erlauben Sie Benutzern, eine Konfigurationsrichtlinie zu erstellen und zu verwalten

Dieses Beispiel zeigt, wie Sie eine IAM-Richtlinie erstellen könnten, die es einem Benutzer ermöglicht, Konfigurationsrichtlinien zu erstellen, anzuzeigen, zu aktualisieren und zu löschen. Diese Beispielrichtlinie ermöglicht es dem Benutzer auch, Richtlinienzuordnungen zu starten, zu beenden und anzuzeigen. Damit diese IAM-Richtlinie funktioniert, muss der Benutzer der delegierte Security Hub-Administrator für eine Organisation sein.

JSON

```
{
```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "CreateAndUpdateConfigurationPolicy",
    "Effect": "Allow",
    "Action": [
      "securityhub:CreateConfigurationPolicy",
      "securityhub:UpdateConfigurationPolicy"
    ],
    "Resource": "*"
  },
  {
    "Sid": "ViewConfigurationPolicy",
    "Effect": "Allow",
    "Action": [
      "securityhub:GetConfigurationPolicy",
      "securityhub:ListConfigurationPolicies"
    ],
    "Resource": "*"
  },
  {
    "Sid": "DeleteConfigurationPolicy",
    "Effect": "Allow",
    "Action": [
      "securityhub:DeleteConfigurationPolicy"
    ],
    "Resource": "*"
  },
  {
    "Sid": "ViewConfigurationPolicyAssociation",
    "Effect": "Allow",
    "Action": [
      "securityhub:BatchGetConfigurationPolicyAssociations",
      "securityhub:GetConfigurationPolicyAssociation",
      "securityhub:ListConfigurationPolicyAssociations"
    ],
    "Resource": "*"
  },
  {
    "Sid": "UpdateConfigurationPolicyAssociation",
    "Effect": "Allow",
    "Action": [
      "securityhub:StartConfigurationPolicyAssociation",
      "securityhub:StartConfigurationPolicyDisassociation"
```

```
    ],  
    "Resource": "*"    
  }  
]  
}
```

Beispiel: Erlauben Sie Benutzern, Ergebnisse einzusehen

Dieses Beispiel zeigt, wie Sie eine IAM-Richtlinie erstellen könnten, die es einem Benutzer ermöglicht, Security Hub Hub-Ergebnisse einzusehen.

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "ReviewFindings",  
      "Effect": "Allow",  
      "Action": [  
        "securityhub:GetFindings"  
      ],  
      "Resource": "*"    
    }  
  ]  
}
```

Beispiel: Erlauben Sie Benutzern, Automatisierungsregeln zu erstellen und zu verwalten

Dieses Beispiel zeigt, wie Sie eine IAM-Richtlinie erstellen könnten, die es einem Benutzer ermöglicht, Security Hub Hub-Automatisierungsregeln zu erstellen, anzuzeigen, zu aktualisieren und zu löschen. Damit diese IAM-Richtlinie funktioniert, muss der Benutzer ein Security Hub-Administrator sein. Um Berechtigungen einzuschränken — z. B. um einem Benutzer zu erlauben, nur Automatisierungsregeln einzusehen — können Sie die Berechtigungen zum Erstellen, Aktualisieren und Löschen entfernen.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateAndUpdateAutomationRules",
      "Effect": "Allow",
      "Action": [
        "securityhub:CreateAutomationRule",
        "securityhub:BatchUpdateAutomationRules"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ViewAutomationRules",
      "Effect": "Allow",
      "Action": [
        "securityhub:BatchGetAutomationRules",
        "securityhub:ListAutomationRules"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DeleteAutomationRules",
      "Effect": "Allow",
      "Action": [
        "securityhub:BatchDeleteAutomationRules"
      ],
      "Resource": "*"
    }
  ]
}
```

Mit Diensten verknüpfte Rollen für AWS Security Hub

AWS Security Hub verwendet eine [dienstverknüpfte AWS Identity and Access Management](#) (IAM) Rolle mit dem Namen `AWSServiceRoleForSecurityHub`. Bei dieser serviceverknüpften Rolle handelt es sich um eine IAM-Rolle, die direkt mit Security Hub verknüpft ist. Es ist von Security Hub vordefiniert und beinhaltet alle Berechtigungen, die Security Hub benötigt, um andere AWS

Ressourcen in Ihrem Namen anzurufen AWS-Services und zu überwachen. Security Hub verwendet diese dienstbezogene Rolle überall dort, AWS-Regionen wo Security Hub verfügbar ist.

Eine serviceverknüpfte Rolle erleichtert die Einrichtung von Security Hub, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Security Hub definiert die Berechtigungen seiner dienstbezogenen Rolle, und sofern die Berechtigungen nicht anders definiert sind, kann nur Security Hub die Rolle übernehmen. Zu den definierten Berechtigungen gehören die Vertrauensrichtlinie und die Berechtigungsrichtlinie, und Sie können diese Berechtigungsrichtlinie keiner anderen IAM-Entität zuordnen.

Um die Details der dienstbezogenen Rolle anzuzeigen, wählen Sie auf der Seite Einstellungen der Security Hub Hub-Konsole Allgemein und dann Dienstberechtigungen anzeigen aus.

Sie können die dienstverknüpfte Security Hub-Rolle erst löschen, nachdem Sie Security Hub zuerst in allen Regionen deaktiviert haben, in denen sie aktiviert ist. Dadurch werden Ihre Security Hub Hub-Ressourcen geschützt, da Sie nicht versehentlich Zugriffsberechtigungen entfernen können.

Informationen zu anderen Diensten, die dienstverknüpfte Rollen unterstützen, finden Sie im IAM-Benutzerhandbuch unter [AWS Dienste, die mit IAM funktionieren](#). Suchen Sie in der Spalte Service-Linked Role nach den Diensten, für die Ja steht. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Themen

- [Dienstbezogene Rollenberechtigungen für Security Hub](#)
- [Eine serviceverknüpfte Rolle für Security Hub erstellen](#)
- [Eine serviceverknüpfte Rolle für Security Hub bearbeiten](#)
- [Löschen einer serviceverknüpften Rolle für Security Hub](#)

Dienstbezogene Rollenberechtigungen für Security Hub

Security Hub verwendet die mit dem Dienst verknüpfte Rolle mit dem Namen `AWSServiceRoleForSecurityHub`. Es handelt sich um eine dienstbezogene Rolle, die für den Zugriff AWS Security Hub auf Ihre Ressourcen erforderlich ist. Die serviceverknüpfte Rolle ermöglicht es Security Hub, Erkenntnisse von anderen zu empfangen AWS-Services und die erforderliche AWS Config Infrastruktur für die Durchführung von Sicherheitsprüfungen für Kontrollen zu konfigurieren.

Die serviceverknüpfte Rolle `AWSServiceRoleForSecurityHub` vertraut darauf, dass die folgenden Services die Rolle annehmen:

- `securityhub.amazonaws.com`

Die serviceverknüpfte Rolle `AWSServiceRoleForSecurityHub` verwendet die verwaltete Richtlinie [AWSSecurityHubServiceRolePolicy](#).

Sie müssen einer IAM-Identität (z. B. einer Rolle, Gruppe oder einem Benutzer) Berechtigungen erteilen, um eine dienstverknüpfte Rolle zu erstellen, zu bearbeiten oder zu löschen. Damit die `AWSServiceRoleForSecurityHub` serviceverknüpfte Rolle erfolgreich erstellt werden kann, muss die IAM-Identität, die Sie für den Zugriff auf Security Hub verwenden, über die erforderlichen Berechtigungen verfügen. Um die erforderlichen Berechtigungen zu gewähren, fügen Sie der Rolle, Gruppe oder dem Benutzer die folgende Richtlinie hinzu.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "securityhub:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "iam:AWSServiceName": "securityhub.amazonaws.com"
        }
      }
    }
  ]
}
```


Eine serviceverknüpfte Rolle für Security Hub erstellen

Die `AWSServiceRoleForSecurityHub` serviceverknüpfte Rolle wird automatisch erstellt, wenn Sie Security Hub zum ersten Mal aktivieren oder Security Hub in einer unterstützten Region aktivieren, in der Sie sie zuvor nicht aktiviert hatten. Sie können die serviceverknüpfte Rolle namens `AWSServiceRoleForSecurityHub` auch manuell erstellen, indem Sie die IAM-Konsole, die CLI oder die IAM-API verwenden.

Important

Die dienstverknüpfte Rolle, die für das Security Hub-Administratorkonto erstellt wurde, gilt nicht für die Security Hub Hub-Mitgliedskonten.

Weitere Informationen zum Erstellen von IAM-Rollen finden Sie unter [Erstellen einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Eine serviceverknüpfte Rolle für Security Hub bearbeiten

Security Hub erlaubt es Ihnen nicht, die `AWSServiceRoleForSecurityHub` dienstverknüpfte Rolle zu bearbeiten. Nachdem Sie eine serviceverknüpfte Rolle erstellt haben, können Sie den Namen der Rolle nicht mehr ändern, da verschiedene Entitäten auf die Rolle verweisen könnten. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter [Bearbeiten einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Security Hub

Wenn Sie ein Feature oder einen Service, die bzw. der eine serviceverknüpfte Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise ist keine ungenutzte Entität vorhanden, die nicht aktiv überwacht oder verwaltet wird.

Important

Um die `AWSServiceRoleForSecurityHub` serviceverknüpfte Rolle zu löschen, müssen Sie Security Hub zunächst in allen Regionen deaktivieren, in denen sie aktiviert ist. Wenn Security Hub nicht deaktiviert ist, wenn Sie versuchen, die serviceverknüpfte Rolle zu löschen, schlägt der Löschvorgang fehl. Weitere Informationen finden Sie unter [Security Hub CSPM deaktivieren](#).

Wenn Sie Security Hub deaktivieren, wird die `AWSServiceRoleForSecurityHub` dienstverknüpfte Rolle nicht automatisch gelöscht. Wenn Sie Security Hub erneut aktivieren, verwendet es ab sofort die bestehende `AWSServiceRoleForSecurityHub` serviceverknüpfte Rolle.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Sie können die IAM-Konsole, die IAM-CLI oder die IAM-API verwenden, um die `AWSServiceRoleForSecurityHub`-serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter [Löschen einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinien für Security Hub

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird. AWS AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie [vom Kunden verwaltete Richtlinien](#) definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter [Von AWS verwaltete Richtlinien](#) im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinie: `AWSSecurityHubFullAccess`

Sie können die `AWSSecurityHubFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Administratorberechtigungen, die einem Principal vollen Zugriff auf alle Security Hub CSPM-Aktionen gewähren. Diese Richtlinie muss einem Prinzipal zugewiesen werden, bevor er Security Hub CSPM manuell für sein Konto aktiviert. Principals mit diesen Berechtigungen können beispielsweise den Status der Ergebnisse sowohl einsehen als auch aktualisieren. Sie können benutzerdefinierte Einblicke konfigurieren und Integrationen aktivieren. Sie können Standards

und Kontrollen aktivieren und deaktivieren. Principals für ein Administratorkonto können auch Mitgliedskonten verwalten.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- **securityhub**— Ermöglicht Principals vollen Zugriff auf alle Security Hub CSPM-Aktionen.
- **guardduty**— Ermöglicht Principals, Informationen über den Kontostatus bei Amazon GuardDuty abzurufen.
- **iam**— Ermöglicht Prinzipalen, eine dienstverknüpfte Rolle für Security Hub CSPM und Security Hub zu erstellen.
- **inspector**— Ermöglicht Principals, Informationen über den Kontostatus in Amazon Inspector abzurufen.
- **pricing**— Ermöglicht Principals, eine Preisliste mit Produkten zu erhalten. AWS-Services

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SecurityHubAllowAll",
      "Effect": "Allow",
      "Action": "securityhub:*",
      "Resource": "*"
    },
    {
      "Sid": "SecurityHubServiceLinkedRole",
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "iam:AWSServiceName": [
            "securityhub.amazonaws.com",
            "securityhubv2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

```

    },
    {
      "Sid": "OtherServicePermission",
      "Effect": "Allow",
      "Action": [
        "guarddduty:GetDetector",
        "guarddduty:ListDetectors",
        "inspector2:BatchGetAccountStatus",
        "pricing:GetProducts"
      ],
      "Resource": "*"
    }
  ]
}

```

Von Security Hub verwaltete CSPM-Richtlinie: AWSSecurityHubReadOnlyAccess

Sie können die AWSSecurityHubReadOnlyAccess-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt nur Leseberechtigungen, die es Benutzern ermöglichen, Informationen in Security Hub CSPM einzusehen. Principals, denen diese Richtlinie beigelegt ist, können keine Updates in Security Hub CSPM vornehmen. Principals mit diesen Berechtigungen können beispielsweise die mit ihrem Konto verknüpfte Ergebnisliste einsehen, den Status eines Fundes jedoch nicht ändern. Sie können die Ergebnisse von Insights einsehen, aber keine benutzerdefinierten Insights erstellen oder konfigurieren. Sie können keine Steuerungen oder Produktintegrationen konfigurieren.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- **securityhub**— Ermöglicht Benutzern das Ausführen von Aktionen, bei denen entweder eine Liste von Elementen oder Details zu einem Artikel zurückgegeben wird. Dazu gehören API-Operationen, die mit `GetList`, oder `beginnenDescribe`.

JSON

```

{
  "Version": "2012-10-17",

```

```
    "Statement": [
      {
        "Sid": "AWSSecurityHubReadOnlyAccess",
        "Effect": "Allow",
        "Action": [
          "securityhub:Get*",
          "securityhub:List*",
          "securityhub:BatchGet*",
          "securityhub:Describe*"
        ],
        "Resource": "*"
      }
    ]
  }
}
```

AWS verwaltete Richtlinie: AWSSecurityHubOrganizationsAccess

Sie können die AWSSecurityHubOrganizationsAccess-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Administratorberechtigungen zur Aktivierung und Verwaltung von Security Hub und Security Hub CSPM innerhalb einer Organisation.

Die Berechtigungen dieser Richtlinie ermöglichen es dem Organisationsverwaltungs-konto, das delegierte Administratorkonto für Security Hub und Security Hub CSPM festzulegen. Sie ermöglichen es dem delegierten Administratorkonto auch, Organisationskonten als Mitgliedskonten zu aktivieren.

Diese Richtlinie stellt nur die Berechtigungen für Organizations bereit. Das Organisationsverwaltungs-konto und das delegierte Administratorkonto benötigen ebenfalls Berechtigungen für zugehörige Aktionen. Diese Berechtigungen können mithilfe der AWSSecurityHubFullAccess verwalteten Richtlinie erteilt werden.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `organizations:ListAccounts`— Ermöglicht Prinzipalen das Abrufen der Liste der Konten, die Teil einer Organisation sind.
- `organizations:DescribeOrganization`— Ermöglicht Prinzipalen das Abrufen von Informationen über die Organisation.

- `organizations:ListRoots`— Ermöglicht Prinzipalen, das Stammverzeichnis einer Organisation aufzulisten.
- `organizations:ListDelegatedAdministrators`— Ermöglicht Prinzipalen, den delegierten Administrator einer Organisation aufzulisten.
- `organizations:ListAWSServiceAccessForOrganization`— Ermöglicht Prinzipalen, diejenigen aufzulisten AWS-Services, die eine Organisation verwendet.
- `organizations:ListOrganizationalUnitsForParent`— Ermöglicht Prinzipalen, die untergeordneten Organisationseinheiten (OU) einer übergeordneten OU aufzulisten.
- `organizations:ListAccountsForParent`— Ermöglicht Prinzipalen, die untergeordneten Konten einer übergeordneten Organisationseinheit aufzulisten.
- `organizations:ListParents`— Führt die Stamm- oder Organisationseinheiten (OUs) auf, die der angegebenen untergeordneten Organisationseinheit oder dem angegebenen untergeordneten Konto als unmittelbare übergeordnete Einheit dienen.
- `organizations:DescribeAccount` – Ermöglicht Prinzipalen den Abruf von Informationen über ein Konto in der Organisation.
- `organizations:DescribeOrganizationalUnit`— Ermöglicht Prinzipalen das Abrufen von Informationen über eine Organisationseinheit in der Organisation.
- `organizations:ListPolicies`— Ruft die Liste aller Richtlinien in einer Organisation eines bestimmten Typs ab.
- `organizations:ListPoliciesForTarget`— Führt die Richtlinien auf, die direkt mit dem angegebenen Zielstamm, der Organisationseinheit (OU) oder dem angegebenen Konto verknüpft sind.
- `organizations:ListTargetsForPolicy`— Führt alle Stammverzeichnisse, Organisationseinheiten (OUs) und Konten auf, denen die angegebene Richtlinie zugeordnet ist.
- `organizations:EnableAWSServiceAccess`— Ermöglicht Prinzipalen, die Integration mit Organizations zu ermöglichen.
- `organizations:RegisterDelegatedAdministrator`— Ermöglicht es den Prinzipalen, das delegierte Administratorkonto festzulegen.
- `organizations:DeregisterDelegatedAdministrator`— Ermöglicht Prinzipalen, das delegierte Administratorkonto zu entfernen.
- `organizations:DescribePolicy`— Ruft Informationen zu einer Richtlinie ab.
- `organizations:DescribeEffectivePolicy`— Gibt den Inhalt der gültigen Richtlinie für den angegebenen Richtlinien Typ und das angegebene Konto zurück.

- `organizations:CreatePolicy`— Erstellt eine Richtlinie eines bestimmten Typs, die Sie einem Stammkonto, einer Organisationseinheit (OU) oder einem einzelnen AWS Konto zuordnen können.
- `organizations:UpdatePolicy`— Aktualisiert eine bestehende Richtlinie mit einem neuen Namen, einer neuen Beschreibung oder einem neuen Inhalt.
- `organizations>DeletePolicy`— Löscht die angegebene Richtlinie aus Ihrer Organisation.
- `organizations:AttachPolicy`— Fügt eine Richtlinie einem Stammkonto, einer Organisationseinheit (OU) oder einem Einzelkonto hinzu.
- `organizations:DetachPolicy`— Trennt eine Richtlinie von einem Zielstamm, einer Organisationseinheit (OU) oder einem Konto.
- `organizations:EnablePolicyType`— Aktiviert einen Richtlinientyp in einem Stamm.
- `organizations:DisablePolicyType`— Deaktiviert einen Organisationsrichtlinientyp in einem Stamm.
- `organizations:TagResource`— Fügt der angegebenen Ressource ein oder mehrere Tags hinzu.
- `organizations:UntagResource`— Entfernt alle Tags mit den angegebenen Schlüsseln aus der angegebenen Ressource.
- `organizations:ListTagsForResource`— Listet Tags auf, die an die angegebene Ressource angehängt sind.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "OrganizationPermissions",
      "Effect": "Allow",
      "Action": [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListRoots",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListParents",

```

```

        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy"
    ],
    "Resource": "*"
},
{
    "Sid": "OrganizationPermissionsEnable",
    "Effect": "Allow",
    "Action": "organizations:EnableAWSServiceAccess",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "organizations:ServicePrincipal": "securityhub.amazonaws.com"
        }
    }
},
{
    "Sid": "OrganizationPermissionsDelegatedAdmin",
    "Effect": "Allow",
    "Action": [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
    ],
    "Resource": "arn:aws:organizations::*:account/o-*/*",
    "Condition": {
        "StringEquals": {
            "organizations:ServicePrincipal":
"securityhub.amazonaws.com"
        }
    }
},
{
    "Sid": "OrganizationPolicyPermissions",
    "Effect": "Allow",
    "Action": [
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:CreatePolicy",
        "organizations:UpdatePolicy",
        "organizations>DeletePolicy",
        "organizations:AttachPolicy",

```



```

        "organizations:DetachPolicy",
        "organizations:EnablePolicyType",
        "organizations:DisablePolicyType"
    ],
    "Resource": [
        "arn:aws:organizations:::root/o-*/**",
        "arn:aws:organizations:::account/o-*/**",
        "arn:aws:organizations:::ou/o-*/**",
        "arn:aws:organizations:::policy/o-*/securityhub_policy/*"
    ],
    "Condition": {
        "StringLikeIfExists": {
            "organizations:PolicyType": "SECURITYHUB_POLICY"
        }
    }
},
{
    "Sid": "OrganizationPolicyTaggingPermissions",
    "Effect": "Allow",
    "Action": [
        "organizations:TagResource",
        "organizations:UntagResource",
        "organizations:ListTagsForResource"
    ],
    "Resource": [
        "arn:aws:organizations:::policy/o-*/securityhub_policy/*"
    ]
}
]
}

```

AWS verwaltete Richtlinie: AWSSecurityHubServiceRolePolicy

Sie können AWSSecurityHubServiceRolePolicy nicht an Ihre IAM-Entitäten anhängen. Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es Security Hub CSPM ermöglicht, Aktionen in Ihrem Namen durchzuführen. Weitere Informationen finden Sie unter [the section called "Service-verknüpfte Rollen"](#).

Diese Richtlinie gewährt Administratorberechtigungen, die es der dienstbezogenen Rolle ermöglichen, die Sicherheitsprüfungen für Security Hub CSPM-Steuerelemente durchzuführen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `cloudtrail`— Ruft Informationen über Wanderwege ab. CloudTrail
- `cloudwatch`— Ruft die aktuellen CloudWatch Alarmer ab.
- `logs`— Ruft die metrischen Filter für CloudWatch Protokolle ab.
- `sns`— Ruft die Liste der Abonnements für ein SNS-Thema ab.
- `config`— Ruft Informationen zu Konfigurationsrekorden, Ressourcen und AWS Config Regeln ab. Ermöglicht der Rolle, die mit dem Service verknüpft ist, außerdem das Erstellen und Löschen von AWS Config Regeln sowie das Ausführen von Evaluierungen anhand der Regeln.
- `iam`— Abrufen und Generieren von Berichten über Anmeldeinformationen für Konten.
- `organizations`— Rufen Sie Informationen zu Konten und Organisationseinheiten (OU) für eine Organisation ab.
- `securityhub`— Rufen Sie Informationen darüber ab, wie der Security Hub CSPM-Dienst, die Standards und die Kontrollen konfiguriert sind.
- `tag`— Ruft Informationen über Ressourcen-Tags ab.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SecurityHubServiceRolePermissions",
      "Effect": "Allow",
      "Action": [
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetEventSelectors",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "logs:DescribeMetricFilters",
        "sns:ListSubscriptionsByTopic",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeConfigRules",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:BatchGetResourceConfig",
        "config:SelectResourceConfig",

```

```

        "iam:GenerateCredentialReport",
        "organizations:ListAccounts",
        "config:PutEvaluations",
        "tag:GetResources",
        "iam:GetCredentialReport",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListChildren",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "securityhub:BatchDisableStandards",
        "securityhub:BatchEnableStandards",
        "securityhub:BatchUpdateStandardsControlAssociations",
        "securityhub:BatchGetSecurityControls",
        "securityhub:BatchGetStandardsControlAssociations",
        "securityhub:CreateMembers",
        "securityhub>DeleteMembers",
        "securityhub:DescribeHub",
        "securityhub:DescribeOrganizationConfiguration",
        "securityhub:DescribeStandards",
        "securityhub:DescribeStandardsControls",
        "securityhub:DisassociateFromAdministratorAccount",
        "securityhub:DisassociateMembers",
        "securityhub:DisableSecurityHub",
        "securityhub:EnableSecurityHub",
        "securityhub:GetEnabledStandards",
        "securityhub:ListStandardsControlAssociations",
        "securityhub:ListSecurityControlDefinitions",
        "securityhub:UpdateOrganizationConfiguration",
        "securityhub:UpdateSecurityControl",
        "securityhub:UpdateSecurityHubConfiguration",
        "securityhub:UpdateStandardsControl",
        "tag:GetResources"
    ],
    "Resource": "*"
},
{
    "Sid": "SecurityHubServiceRoleConfigPermissions",
    "Effect": "Allow",
    "Action": [
        "config:PutConfigRule",
        "config>DeleteConfigRule",
        "config:GetComplianceDetailsByConfigRule"
    ],

```

```

        "Resource": "arn:aws:config:*:*:config-rule/aws-service-rule/
*securityhub*"
    },
    {
        "Sid": "SecurityHubServiceRoleOrganizationsPermissions",
        "Effect": "Allow",
        "Action": [
            "organizations:ListDelegatedAdministrators"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "organizations:ServicePrincipal": [
                    "securityhub.amazonaws.com"
                ]
            }
        }
    }
}
]
}

```

AWS verwaltete Richtlinie: AWSSecurityHubV2ServiceRolePolicy

Note

Security Hub befindet sich in der Vorschauversion und kann sich ändern.

Diese Richtlinie ermöglicht es Security Hub, AWS Config Regeln und Security Hub Hub-Ressourcen in Ihrer Organisation und in Ihrem Namen zu verwalten. Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen. Weitere Informationen finden Sie unter [the section called “Service-verknüpfte Rollen”](#).

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- **config**— Verwaltet serviceverknüpfte Konfigurationsrekorder für Security Hub Hub-Ressourcen.
- **iam**— Erstellt die serviceverknüpfte Rolle für AWS Config

- **organizations**— Ruft Informationen zu Konten und Organisationseinheiten (OU) für eine Organisation ab.
- **securityhub**— Verwaltet die Security Hub Hub-Konfiguration.
- **tag**— Ruft Informationen über Ressourcen-Tags ab.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SecurityHubV2ServiceRoleAssetsConfig",
      "Effect": "Allow",
      "Action": [
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:PutServiceLinkedConfigurationRecorder"
      ],
      "Resource": "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForSecurityHubAssets/*"
    },
    {
      "Sid": "SecurityHubV2ServiceRoleAssetsIamPermissions",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "arn:aws:iam:*:*:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "config.amazonaws.com"
        }
      }
    },
    {
      "Sid": "SecurityHubV2ServiceRoleSecurityHubPermissions",
      "Effect": "Allow",
      "Action": [
        "securityhub:DisableSecurityHubV2",
```

```

        "securityhub:EnableSecurityHubV2",
        "securityhub:DescribeSecurityHubV2"
    ],
    "Resource": "arn:aws:securityhub:*:*:hubv2/*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
    }
},
{
    "Sid": "SecurityHubV2ServiceRoleTagPermissions",
    "Effect": "Allow",
    "Action": [
        "tag:GetResources"
    ],
    "Resource": "*"
},
{
    "Sid": "SecurityHubV2ServiceRoleOrganizationsPermissionsOnResources",
    "Effect": "Allow",
    "Action": [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit"
    ],
    "Resource": "arn:aws:organizations:*:*:*"
},
{
    "Sid":
"SecurityHubV2ServiceRoleOrganizationsPermissionsWithoutResources",
    "Effect": "Allow",
    "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren"
    ],
    "Resource": "*"
},
{
    "Sid": "SecurityHubV2ServiceRoleDelegatedAdminPermissions",
    "Effect": "Allow",
    "Action": [
        "organizations:ListDelegatedAdministrators"
    ]
}

```

```
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "organizations:ServicePrincipal": [
          "securityhub.amazonaws.com"
        ]
      }
    }
  }
}
```

Security Hub CSPM-Updates für verwaltete Richtlinien AWS

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Security Hub CSPM an, seit dieser Dienst begonnen hat, diese Änderungen zu verfolgen. Abonnieren Sie den RSS-Feed auf der Seite [CSPM-Dokumentenverlauf](#) von Security Hub, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.

Änderung	Beschreibung	Datum
AWSSecurityHubOrganizationsAccess – Aktualisierung auf eine bestehende Richtlinie	Security Hub CSPM hat eine neue Berechtigung hinzugefügt. <code>AWSSecurityHubOrganizationsAccess</code> Die Berechtigung ermöglicht es der Unternehmensleitung, Security Hub und Security Hub CSPM innerhalb einer Organisation zu aktivieren und zu verwalten.	17. Juni 2025
AWSSecurityHubOrganizationsAccess – Aktualisierung auf eine bestehende Richtlinie	Es wurden neue Berechtigungen hinzugefügt, die es der Unternehmensleitung ermöglichen, Security Hub und	17. Juni 2025

Änderung	Beschreibung	Datum
	Security Hub CSPM innerhalb einer Organisation zu aktivieren und zu verwalten.	
AWSSecurityHubFullAccess – Aktualisierung auf eine bestehende Richtlinie	Security Hub CSPM hat eine neue Berechtigung hinzugefügt, die es Prinzipal en ermöglicht, eine dienstbezogene Rolle für Security Hub zu erstellen.	17. Juni 2025
AWSSecurityHubV2ServiceRolePolicy — Neue Richtlinie	Security Hub hat eine neue Richtlinie hinzugefügt, die es Security Hub ermöglicht, AWS Config Regeln und Security Hub Hub-Ressourcen in der Organisation eines Kunden und im Namen des Kunden zu verwalten. Security Hub befindet sich in der Vorschauversion und kann sich ändern.	17. Juni 2025
AWSSecurityHubFullAccess — Aktualisierung einer bestehenden Richtlinie	Security Hub CSPM hat die Richtlinie aktualisiert, um Preisdetails für AWS-Services und Produkte zu erhalten.	24. April 2024
AWSSecurityHubReadOnlyAccess — Aktualisierung einer bestehenden Richtlinie	Security Hub CSPM hat diese verwaltete Richtlinie aktualisiert, indem ein <code>Sid</code> Feld hinzugefügt wurde.	22. Februar 2024

Änderung	Beschreibung	Datum
AWSSecurityHubFullAccess — Aktualisierung einer bestehenden Richtlinie	Security Hub CSPM hat die Richtlinie aktualisiert, sodass festgestellt werden kann, ob Amazon GuardDuty und Amazon Inspector in einem Konto aktiviert sind. Dies hilft Kunden dabei, sicherheitsrelevante Informationen aus mehreren zusammenzuführen. AWS-Services	16. November 2023
AWSSecurityHubOrganizationsAccess — Aktualisierung einer bestehenden Richtlinie	Security Hub CSPM hat die Richtlinie aktualisiert, um zusätzliche Berechtigungen für den schreibgeschützten Zugriff auf delegierte Administratorfunktionen zu AWS Organizations gewähren. Dazu gehören Details wie das Stammverzeichnis, die Organisationseinheiten (OUs), die Konten, die Organisationsstruktur und der Dienstzugriff.	16. November 2023

Änderung	Beschreibung	Datum
AWSSecurityHubServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Security Hub CSPM hat die <code>UpdateSecurityControl</code> Berechtigungen <code>BatchGetSecurityControls</code> <code>DisassociateFromAdministratorAccount</code> , und zum Lesen und Aktualisieren anpassbarer Sicherheitskontrolleigenschaften hinzugefügt.	26. November 2023
AWSSecurityHubServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Security Hub CSPM hat die <code>tag:GetResources</code> Erlaubnis hinzugefügt, Ressourcen-Tags zu lesen, die sich auf Ergebnisse beziehen.	7. November 2023
AWSSecurityHubServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Security Hub CSPM hat die <code>BatchGetStandardsControlAssociations</code> Erlaubnis hinzugefügt, Informationen über den Aktivierungsstatus eines Steuerelements in einem Standard abzurufen.	27. September 2023

Änderung	Beschreibung	Datum
AWSSecurityHubServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Security Hub CSPM hat neue Berechtigungen zum Abrufen von AWS Organizations Daten sowie zum Lesen und Aktualisieren von Security Hub CSPM-Konfigurationen, einschließlich Standards und Kontrollen, hinzugefügt.	20. September 2023
AWSSecurityHubServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Security Hub CSPM hat die bestehende <code>config:DescribeConfigRuleEvaluationStatus</code> Berechtigung in eine andere Erklärung innerhalb der Richtlinie verschoben. Die <code>config:DescribeConfigRuleEvaluationStatus</code> Erlaubnis wird jetzt auf alle Ressourcen angewendet.	17. März 2023
AWSSecurityHubServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Security Hub CSPM hat die bestehende <code>config:PutEvaluation</code> Berechtigung in eine andere Erklärung innerhalb der Richtlinie verschoben. Die <code>config:PutEvaluation</code> Erlaubnis wird jetzt auf alle Ressourcen angewendet.	14. Juli 2021

Änderung	Beschreibung	Datum
AWSSecurityHubServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Security Hub CSPM hat eine neue Berechtigung hinzugefügt, die es der serviceverknüpften Rolle ermöglicht, Bewertungsergebnisse zu liefern. AWS Config	29. Juni 2021
AWSSecurityHubServiceRolePolicy — Zur Liste der verwalteten Richtlinien hinzugefügt	Es wurden Informationen zur verwalteten Richtlinie hinzugefügt AWSSecurityHubServiceRolePolicy, die von der serviceverknüpften Rolle Security Hub CSPM verwendet wird.	11. Juni 2021
AWSSecurityHubOrganizationsAccess — Neue Richtlinie	Security Hub CSPM hat eine neue Richtlinie hinzugefügt, die Berechtigungen gewährt, die für die Security Hub CSPM-Integration mit Organizations erforderlich sind.	15. März 2021
Security Hub CSPM hat begonnen, Änderungen zu verfolgen	Security Hub CSPM begann, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	15. März 2021

Fehlerbehebung bei AWS Security Hub Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit AWS Security Hub IAM auftreten können.

Themen

- [Ich bin nicht berechtigt, eine Aktion in Security Hub durchzuführen](#)

- [Ich bin nicht berechtigt, iam auszuführen: PassRole](#)
- [Ich möchte programmatischen Zugriff auf Security Hub](#)
- [Ich bin Administrator und möchte anderen den Zugriff auf Security Hub ermöglichen](#)
- [Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Security Hub Hub-Ressourcen ermöglichen](#)

Ich bin nicht berechtigt, eine Aktion in Security Hub durchzuführen

Wenn Ihnen AWS Management Console mitgeteilt wird, dass Sie nicht berechtigt sind, eine Aktion durchzuführen, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Der folgende Beispielfehler tritt auf, wenn der Benutzer `mateojackson` versucht, die Konsole zu verwenden, um Details zu einem anzuzeigen, `widget` aber nicht über die `securityhub:GetWidget` entsprechenden Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
securityhub:GetWidget on resource: my-example-widget
```

In diesem Fall bittet Mateo seinen Administrator um die Aktualisierung seiner Richtlinien, um unter Verwendung der Aktion `my-example-widget` auf die Ressource `securityhub:GetWidget` zugreifen zu können.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die `iam:PassRole` Aktion durchzuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an Security Hub übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Security Hub auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion iam:PassRole ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte programmatischen Zugriff auf Security Hub

Benutzer benötigen programmatischen Zugriff, wenn sie mit AWS außerhalb des interagieren möchten. AWS Management Console Die Art und Weise, wie programmatischer Zugriff gewährt wird, hängt vom Benutzertyp ab, der zugreift. AWS

Um Benutzern programmgesteuerten Zugriff zu gewähren, wählen Sie eine der folgenden Optionen.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
Mitarbeiteridentität (Benutzer, die in IAM Identity Center verwaltet werden)	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an das AWS CLI AWS SDKs, oder zu signieren. AWS APIs	Befolgen Sie die Anweisung en für die Schnittstelle, die Sie verwenden möchten. • Informationen zu den AWS CLI finden Sie unter Konfiguration der AWS CLI zur Verwendung AWS IAM Identity Center im AWS Command Line Interface Benutzerhandbuch. • Informationen zu AWS SDKs Tools und AWS APIs finden Sie unter IAM Identity Center-Authentifizierung im Referenzhandbuch AWS SDKs und im Tools-Referenzhandbuch.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
IAM	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an das AWS CLI AWS SDKs, oder zu signieren. AWS APIs	Folgen Sie den Anweisungen unter Verwenden temporärer Anmeldeinformationen mit AWS Ressourcen im IAM-Benutzerhandbuch.
IAM	(Nicht empfohlen) Verwenden Sie langfristige Anmeldeinformationen, um programmatische Anfragen an das AWS CLI AWS SDKs, oder zu signieren. AWS APIs	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen dazu AWS CLI finden Sie unter Authentifizierung mithilfe von IAM-Benutzeranmeldinformationen im AWS Command Line Interface Benutzerhandbuch. • Informationen zu AWS SDKs und Tools finden Sie unter Authentifizieren mit langfristigen Anmeldeinformationen im Referenzhandbuch AWS SDKs und im Tools-Referenzhandbuch. • Weitere Informationen finden Sie unter Verwaltung von Zugriffsschlüsseln für IAM-Benutzer im IAM-Benutzerhandbuch. AWS APIs

Ich bin Administrator und möchte anderen den Zugriff auf Security Hub ermöglichen

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

- Benutzer und Gruppen in AWS IAM Identity Center:

Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter [Erstellen eines Berechtigungssatzes](#) im AWS IAM Identity Center -Benutzerhandbuch.

- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anleitung unter [Eine Rolle für einen externen Identitätsanbieter \(Verbund\) erstellen](#) im IAM-Benutzerhandbuch.

- IAM-Benutzer:

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

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Security Hub Hub-Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob Security Hub diese Funktionen unterstützt, finden Sie unter [So funktioniert Security Hub mit IAM](#).
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im [IAM-Benutzerhandbuch unter Zugriff auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen](#).
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie [AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte](#).
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter [Gewähren von Zugriff für extern authentifizierte Benutzer \(Identitätsverbund\)](#) im IAM-Benutzerhandbuch.

- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [Kontoübergreifender Ressourcenzugriff in IAM](#) im IAM-Benutzerhandbuch.

Compliance-Validierung für AWS Security Hub

Um zu erfahren, ob AWS-Service ein in den Geltungsbereich bestimmter Compliance-Programme fällt, siehe [AWS-Services in Geltungsbereich nach Compliance-Programm AWS-Services](#) und wählen Sie das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter [AWS Compliance-Programme AWS](#).

Die Auditberichte von Drittanbietern lassen sich mit herunterlade AWS Artifact. Weitere Informationen finden Sie unter [Herunterladen von Berichten in AWS Artifact](#).

Ihre Compliance-Verantwortung bei Verwendung AWS-Services hängt von der Vertraulichkeit der Daten, den Compliance-Zielen des Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen bereit, um Sie bei der Compliance zu unterstützen:

- [Compliance und Governance im Bereich Sicherheit](#) – In diesen Anleitungen für die Lösungsimplementierung werden Überlegungen zur Architektur behandelt. Außerdem werden Schritte für die Bereitstellung von Sicherheits- und Compliance-Features beschrieben.
- [Referenz für berechnete HIPAA-Services](#) – Listet berechnete HIPAA-Services auf. Nicht alle AWS-Services sind HIPAA-berechtigt.
- [AWS](#) — Diese Arbeitsbücher und Leitfäden könnten für Ihre Branche und Ihren Standort relevant sein.
- [AWS -Compliance-Leitfäden für Kunden](#) — Verstehen Sie das Modell der geteilten Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Methoden zum Schutz von zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO) zugeordnet.
- [Auswertung von Ressourcen mit Regeln](#) im AWS Config Entwicklerhandbuch — Der AWS Config -Service bewertet, wie gut Ihre Ressourcenkonfigurationen mit internen Praktiken, Branchenrichtlinien und Vorschriften übereinstimmen.
- [AWS Security Hub](#) — Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um

Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Die Liste der unterstützten Services und Kontrollen finden Sie in der [Security-Hub-Steuerelementreferenz](#).

- [Amazon GuardDuty](#) — Dieser AWS-Service erkennt potenzielle Bedrohungen für Ihre AWS-Konten, Workloads, Container und Daten, indem er Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedenen Compliance-Anforderungen wie PCI DSS nachzukommen, indem es die Anforderungen zur Erkennung von Eindringlingen erfüllt, die in bestimmten Compliance-Frameworks vorgeschrieben sind.
- [AWS Audit Manager](#) — Dieser AWS-Service hilft Ihnen, Ihre AWS -Nutzung kontinuierlich zu überprüfen, um zu vereinfachen, wie Sie mit Risiken umgehen und Compliance sowie Branchenstandards einhalten.

Resilienz im AWS Security Hub

Die AWS globale Infrastruktur basiert auf Availability AWS-Regionen Zones. Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die über hoch redundante Netzwerke mit niedriger Latenz und hohen Durchsätzen verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter [AWS Globale Infrastruktur](#).

Infrastruktursicherheit in AWS Security Hub

Als verwalteter Dienst AWS Security Hub ist er durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter [AWS Cloud-Sicherheit](#). Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter [Infrastructure Protection](#) in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Security Hub zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.

- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit [AWS Security Token Service](#) (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

AWS Security Hub und Schnittstellen-VPC-Endpunkte (AWS PrivateLink)

Sie können eine private Verbindung zwischen Ihrer VPC und erstellen, AWS Security Hub indem Sie einen Schnittstellen-VPC-Endpunkt erstellen. Die Schnittstellen-Endpunkte werden mit bereitgestellt [AWS PrivateLink](#), einer Technologie, die es Ihnen ermöglicht, APIs ohne Internet-Gateway, NAT-Gerät, VPN-Verbindung oder AWS Direct-Connect-Verbindung privat auf Security Hub zuzugreifen. Die Instances in Ihrer VPC benötigen für die Kommunikation mit Security Hub APIs keine öffentlichen IP-Adressen. Der Datenverkehr zwischen Ihrer VPC und Security Hub verlässt das Amazon-Netzwerk nicht.

Jeder Schnittstellenendpunkt wird durch eine oder mehrere [Elastic-Netzwerk-Schnittstellen](#) in Ihren Subnetzen dargestellt. Weitere Informationen finden Sie unter [Zugreifen und AWS-Service Verwenden eines VPC-Endpunkts mit einer Schnittstelle](#) im Amazon Virtual Private Cloud Guide.

Überlegungen zu Security Hub Hub-VPC-Endpunkten

Bevor Sie einen Schnittstellen-VPC-Endpunkt für Security Hub einrichten, informieren Sie sich über die Voraussetzungen und weitere Informationen im [Amazon Virtual Private Cloud Cloud-Handbuch](#).

Security Hub unterstützt Aufrufe all seiner API-Aktionen aus Ihrer VPC.

Erstellen eines Schnittstellen-VPC-Endpunkts für Security Hub

Sie können einen VPC-Endpunkt für den Security Hub-Service mithilfe der Amazon-VPC-Konsole oder der AWS Command Line Interface (AWS CLI) erstellen. Weitere Informationen finden Sie unter [Erstellen eines VPC-Endpunkts](#) im Amazon Virtual Private Cloud Cloud-Handbuch.

Erstellen Sie einen VPC-Endpunkt für Security Hub mit dem folgenden Servicenamen:

`com.amazonaws.region.securityhub`

Wo *region* ist der Regionalcode für den AWS-Region zutreffenden.

Wenn Sie einen privaten DNS für den Endpunkt aktivieren, können Sie mittels seines standardmäßigen DNS-Namen für die Region, beispielsweise für die Region USA Ost (Nord-Virginia), `securityhub.us-east-1.amazonaws.com` API-Anforderungen an Security Hub senden.

Erstellen einer VPC-Endpunktrichtlinie für Security Hub

Sie können eine Endpunktrichtlinie an Ihren VPC-Endpunkt anhängen, der den Zugriff auf Security Hub steuert. Die Richtlinie gibt die folgenden Informationen an:

- Prinzipal, der die Aktionen ausführen kann.
- Aktionen, die ausgeführt werden können
- Die Ressourcen, für die Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter [Steuern des Zugriffs auf VPC-Endpunkte mithilfe von Endpunktrichtlinien](#) im Amazon Virtual Private Cloud Cloud-Handbuch.

Beispiel: VPC-Endpunktrichtlinie für Security Hub Hub-Aktionen

Im Folgenden finden Sie ein Beispiel für eine Endpunktrichtlinie für Security Hub. Wenn diese Richtlinie an einen Endpunkt angefügt wird, gewährt sie Zugriff auf die aufgelisteten Security Hub Hub-Aktionen für alle Prinzipale auf allen Ressourcen.

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "securityhub:getFindings",
        "securityhub:getEnabledStandards",
        "securityhub:getInsights"
      ],
      "Resource": "*"
    }
  ]
}
```

Gemeinsam genutzte Subnetze

Sie können VPC-Endpunkte in Subnetzen, die mit Ihnen geteilt werden, nicht erstellen, beschreiben, ändern oder löschen. Sie können die VPC-Endpunkte jedoch in Subnetzen verwenden, die mit Ihnen geteilt werden. Informationen zur VPC-Freigabe finden Sie unter [Freigeben Ihrer VPC-Subnetze für andere Konten im Leitfaden für Amazon Virtual Private Cloud](#).

Security Hub CSPM-API-Aufrufe protokollieren mit CloudTrail

AWS Security Hub Cloud Security Posture Management (CSPM) ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen eines Benutzers, einer Rolle oder eines AWS Dienstes in Security Hub CSPM bereitstellt. CloudTrail erfasst API-Aufrufe für Security Hub CSPM als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Security Hub CSPM-Konsole und Code-Aufrufe an die Security Hub CSPM-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Security Hub CSPM. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem auf der CloudTrail Konsole im Ereignisverlauf einsehen. Anhand der CloudTrail gesammelten Informationen können Sie die Anfrage, die an Security Hub CSPM gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen darüber CloudTrail, einschließlich der Konfiguration und Aktivierung, finden Sie im [AWS CloudTrail Benutzerhandbuch](#).

Security Hub CSPM-Informationen in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn unterstützte Ereignisaktivitäten in Security Hub CSPM auftreten, wird diese Aktivität zusammen mit anderen AWS Dienstereignissen im CloudTrail Ereignisverlauf in einem Ereignis aufgezeichnet. Sie können die neusten Ereignisse in Ihr -Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter [Ereignisse mit CloudTrail Ereignisverlauf anzeigen](#).

Für eine fortlaufende Aufzeichnung von Ereignissen in Ihrem Konto, einschließlich Ereignissen für Security Hub CSPM, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Standardmäßig gilt ein in der Konsole erstellter Trail für alle AWS -Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- [Übersicht zum Erstellen eines Trails](#)

- [CloudTrail unterstützte Dienste und Integrationen](#)
- [Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail](#)
- [Empfangen von CloudTrail Protokolldateien aus mehreren Regionen](#) und [Empfangen von CloudTrail Protokolldateien von mehreren Konten](#)

Security Hub CSPM unterstützt die Protokollierung aller Security Hub CSPM-API-Aktionen als Ereignisse in Protokollen. CloudTrail Eine Liste der Security Hub CSPM-Operationen finden Sie in der [Security Hub CSPM API-Referenz](#).

Wenn Aktivitäten für die folgenden Aktionen protokolliert werden CloudTrail, ist der Wert für `responseElements` auf gesetzt. `null` Dadurch wird sichergestellt, dass vertrauliche Informationen nicht in den CloudTrail Protokollen enthalten sind.

- `BatchImportFindings`
- `GetFindings`
- `GetInsights`
- `GetMembers`
- `UpdateFindings`

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde
- Ob die Anfrage mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen föderierten Benutzer ausgeführt wurde
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde

Weitere Informationen finden Sie unter [CloudTrail -Element userIdentity](#).

Beispiel: Security Hub CSPM-Protokolldateieinträge

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen

Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die CreateInsight Aktion demonstriert. In diesem Beispiel wird ein Insight mit dem Namen Test Insight erstellt. Das ResourceId Attribut ist als Gruppieren nach Aggregator angegeben, und es wurden keine optionalen Filter für diesen Einblick angegeben. Weitere Informationen über Funde sind unter [Einblicke in Security Hub CSPM anzeigen](#) verfügbar.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAJK6U5DS22IAVUI7BW",
    "arn": "arn:aws:iam::012345678901:user/TestUser",
    "accountId": "012345678901",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "TestUser"
  },
  "eventTime": "2018-11-25T01:02:18Z",
  "eventSource": "securityhub.amazonaws.com",
  "eventName": "CreateInsight",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "205.251.233.179",
  "userAgent": "aws-cli/1.11.76 Python/2.7.10 Darwin/17.7.0 botocore/1.5.39",
  "requestParameters": {
    "Filters": {},
    "ResultField": "ResourceId",
    "Name": "Test Insight"
  },
  "responseElements": {
    "InsightArn": "arn:aws:securityhub:us-west-2:0123456789010:insight/custom/f4c4890b-ac6b-4c26-95f9-e62cc46f3055"
  },
  "requestID": "c0ffffccd-f04d-11e8-93fc-ddcd14710066",
  "eventID": "3dabcebf-35b0-443f-a1a2-26e186ce23bf",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "recipientAccountId": "012345678901"
}
```


Kennzeichnung von Security Hub CSPM-Ressourcen

Ein Tag ist eine optionale Bezeichnung, die Sie definieren und AWS Ressourcen zuweisen können, einschließlich bestimmter Typen von AWS Security Hub Cloud Security Posture Management (CSPM) -Ressourcen. Mithilfe von Tags können Sie Ressourcen auf unterschiedliche Weise identifizieren, kategorisieren und verwalten, z. B. nach Zweck, Eigentümer, Umgebung oder anderen Kriterien. Mithilfe von Tags können Sie beispielsweise zwischen Ressourcen unterscheiden, Ressourcen identifizieren, die bestimmte Compliance-Anforderungen oder Workflows unterstützen, oder Kosten zuordnen.

Sie können Tags zu den folgenden Typen von Security Hub CSPM-Ressourcen hinzufügen:

- Regeln für die Automatisierung
- Konfigurationsrichtlinien
- Hub-Ressource

Grundlagen des Kennzeichnens

Eine Ressource kann bis zu 50 Tags enthalten. Jedes Tag besteht aus einem Schlüssel und einem optionalen Wert. Beides können Sie definieren. Ein Tag-Schlüssel ist eine allgemeine Bezeichnung, die als Kategorie für einen spezifischeren Tag-Wert dient. Ein Tag-Wert dient als Bezeichnung für einen Tag-Schlüssel.

Wenn Sie beispielsweise unterschiedliche Automatisierungsregeln für verschiedene Umgebungen erstellen (einen Satz von Automatisierungsregeln für Testkonten und einen anderen für Produktionskonten), können Sie diesen Regeln einen Environment Tagschlüssel zuweisen. Der zugehörige Tagwert kann Test für die Regeln gelten, die Testkonten zugeordnet sind, und Prod für die Regeln, die Produktionskonten und zugeordnet sind OUs.

Beachten Sie bei der Definition und Zuweisung von Tags zu AWS Security Hub Cloud Security Posture Management (CSPM) -Ressourcen Folgendes:

- Jede Ressource kann maximal 50 Tags haben.
- Für jede Ressource muss jeder Tag-Schlüssel eindeutig sein und er kann nur einen Tag-Wert haben.

- Bei Tag-Schlüsseln und -Werten muss die Groß- und Kleinschreibung beachtet werden. Als bewährte Methode empfehlen wir Ihnen, eine Strategie zur Großschreibung von Tags zu definieren und diese Strategie in allen Ressourcen einheitlich umzusetzen.
- Ein Tag-Schlüssel kann maximal 128 UTF-8-Zeichen enthalten. Ein Tag-Wert kann maximal 256 UTF-8-Zeichen enthalten. Bei den Zeichen kann es sich um Buchstaben, Zahlen, Leerzeichen oder die folgenden Symbole handeln: `_` `./` `=` `+` `-` `@`
- Das `aws :` Präfix ist für die Verwendung durch reserviert AWS. Sie können es nicht in Tag-Schlüsseln oder -Werten verwenden, die Sie definieren. Außerdem können Sie Tag-Schlüssel oder -Werte, die dieses Präfix verwenden, nicht ändern oder entfernen. Tags mit diesem Präfix werden beim Kontingent von 50 Tags pro Ressource nicht eingerechnet.
- Alle Tags, die Sie zuweisen, sind nur für Sie AWS-Konto und nur in dem verfügbar, AWS-Region in dem Sie sie zuweisen.
- Wenn Sie einer Ressource mithilfe von Security Hub CSPM Tags zuweisen, werden die Tags nur auf die Ressource angewendet, die direkt im Security Hub CSPM im entsprechenden Verzeichnis gespeichert ist. AWS-Region Sie gelten nicht für zugehörige, unterstützende Ressourcen, die Security Hub CSPM für Sie in anderen Bereichen erstellt, verwendet oder verwaltet. AWS-Services Wenn Sie beispielsweise einer Automatisierungsregel, die Ergebnisse im Zusammenhang mit Amazon Simple Storage Service (Amazon S3) aktualisiert, Tags zuweisen, werden die Tags nur auf Ihre Automatisierungsregel in Security Hub CSPM für die angegebene Region angewendet. Sie werden nicht auf Ihre S3-Buckets angewendet. Um auch einer zugehörigen Ressource Tags zuzuweisen, können Sie AWS Resource Groups oder das verwenden, in dem AWS-Service die Ressource gespeichert ist, z. B. Amazon S3 für einen S3-Bucket. Das Zuweisen von Tags zu zugehörigen Ressourcen kann Ihnen dabei helfen, unterstützende Ressourcen für Ihre Security Hub CSPM-Ressourcen zu identifizieren.
- Wenn Sie eine Ressource löschen, werden alle Tags, die der Ressource zugewiesen sind, ebenfalls gelöscht.

 Important

Speichern Sie keine vertraulichen oder anderen sensiblen Daten in Tags. Auf Tags kann von vielen aus zugegriffen werden AWS-Services, darunter AWS Fakturierung und Kostenmanagement. Sie sind nicht dafür vorgesehen, für sensible Daten verwendet zu werden.

Um Tags für Security Hub CSPM-Ressourcen hinzuzufügen und zu verwalten, können Sie die Security Hub CSPM-Konsole, die Security Hub CSPM API oder die Tagging API verwenden. AWS Resource Groups Mit Security Hub CSPM können Sie einer Ressource Tags hinzufügen, wenn Sie die Ressource erstellen. Sie können auch Tags für einzelne vorhandene Ressourcen hinzufügen und verwalten. Mit Resource Groups können Sie Tags für mehrere bestehende Ressourcen, einschließlich Security Hub CSPM AWS-Services, in großen Mengen hinzufügen und verwalten.

Weitere Tipps und bewährte Methoden zur Kennzeichnung finden Sie unter [Tagging Your AWS Resources User Guide im Tagging Resources](#) User Guide. AWS

Verwenden von Tags in IAM-Richtlinien

Nachdem Sie mit dem Taggen von Ressourcen begonnen haben, können Sie tagbasierte Berechtigungen auf Ressourcenebene in (IAM-) Richtlinien definieren. AWS Identity and Access Management Durch die Verwendung von Tags auf diese Weise können Sie detailliert steuern, welche Benutzer und Rollen in Ihrem Unternehmen die Berechtigung AWS-Konto haben, Ressourcen zu erstellen und zu taggen, und welche Benutzer und Rollen generell die Berechtigung haben, Tags hinzuzufügen, zu bearbeiten und zu entfernen. Um den Zugriff anhand von Tags zu steuern, können Sie im [Element Condition der IAM-Richtlinien Tag-bezogene Bedingungsschlüssel](#) verwenden.

Sie können beispielsweise eine IAM-Richtlinie erstellen, die einem Benutzer vollen Zugriff auf alle AWS Security Hub Cloud Security Posture Management (CSPM) -Ressourcen gewährt, wenn das Owner Tag für die Ressource seinen Benutzernamen angibt:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ModifyResourceIfOwner",
      "Effect": "Allow",
      "Action": "securityhub:*",
      "Resource": "*",
      "Condition": {
        "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner":
"${aws:username}"}
      }
    }
  ]
}
```

```
]
}
```

Wenn Sie Tag-basierte Berechtigungen auf Ressourcenebene definieren, werden die Berechtigungen sofort wirksam. Dies bedeutet, dass Ihre Ressourcen besser geschützt sind, sobald sie erstellt wurden, und Sie schnell damit beginnen können, die Verwendung von Tags für neue Ressourcen zu erzwingen. Mithilfe von Berechtigungen auf Ressourcenebene können Sie auch steuern, welche Tag-Schlüssel und -Werte können mit neuen und vorhandenen Ressourcen verknüpft werden können. Weitere Informationen finden Sie unter [Steuern des Zugriffs auf AWS Ressourcen mithilfe von Tags](#) im IAM-Benutzerhandbuch.

Hinzufügen von Tags zu Security Hub CSPM-Ressourcen

Ein Tag ist eine Bezeichnung, die Sie definieren und AWS Ressourcen zuweisen können, einschließlich bestimmter Typen von AWS Security Hub Cloud Security Posture Management (CSPM) -Ressourcen. Mithilfe von Tags können Sie Ressourcen auf unterschiedliche Weise identifizieren, kategorisieren und verwalten, z. B. nach Zweck, Eigentümer, Umgebung oder anderen Kriterien. Sie können Tags beispielsweise verwenden, um Richtlinien anzuwenden, Kosten zuzuweisen, zwischen Versionen von Ressourcen zu unterscheiden oder Ressourcen zu identifizieren, die bestimmte Compliance-Anforderungen oder Workflows unterstützen.

Sie können Tags zu den folgenden Typen von Security Hub CSPM-Ressourcen hinzufügen:

- Regeln für die Automatisierung
- Konfigurationsrichtlinien
- Hub-Ressource

Eine Ressource kann bis zu 50 Tags enthalten. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Ein Tag-Schlüssel ist eine allgemeine Bezeichnung, die als Kategorie für einen spezifischeren Tag-Wert dient. Ein Tag-Wert dient als Bezeichnung für einen Tag-Schlüssel. Weitere Informationen zu Tag-Optionen und Anforderungen finden Sie unter [Grundlagen des Kennzeichnens](#).

Um einer Security Hub CSPM-Ressource Tags hinzuzufügen, können Sie die Security Hub CSPM-Konsole oder die Security Hub CSPM-API verwenden. Die Konsole unterstützt jedoch nicht das Hinzufügen von Tags zur Ressource. Hub

Nachdem Sie Tags hinzugefügt haben, können Sie das Tag bearbeiten und den Tag-Schlüssel oder den Tag-Wert ändern.

[Verwenden Sie die Tagging-Operationen der Tagging-API, um Tags für mehrere Security Hub CSPM-Ressourcen gleichzeitig hinzuzufügen oder zu bearbeiten.](#)[AWS Resource Groups](#)

 Important

Das Hinzufügen von Tags zu einer Ressource kann sich auf den Zugriff auf die Ressource auswirken. Bevor Sie einer Ressource ein Tag hinzufügen, überprüfen Sie alle AWS Identity and Access Management (IAM-) Richtlinien, die möglicherweise Tags verwenden, um den Zugriff auf Ressourcen zu steuern.

Console

So fügen Sie einer Security Hub CSPM-Ressource (Konsole) Tags hinzu

Wenn Sie eine Automatisierungsregel oder eine Konfigurationsrichtlinie erstellen, bietet die Security Hub CSPM-Konsole Optionen zum Hinzufügen von Tags. Sie können den Tag-Schlüssel und den Tag-Wert im Abschnitt Tags angeben.

Security Hub CSPM API

So fügen Sie einer Security Hub CSPM-Ressource (API) Tags hinzu

Um eine Ressource zu erstellen und ihr programmgesteuert ein oder mehrere Tags hinzuzufügen, verwenden Sie die entsprechende Operation für den Ressourcentyp, den Sie erstellen möchten:

- Um eine Konfigurationsrichtlinie zu erstellen und ihr ein oder mehrere Tags hinzuzufügen, rufen Sie die [CreateConfigurationPolicy](#)API auf oder führen Sie, falls Sie die verwenden AWS CLI, den Befehl aus. [create-configuration-policy](#)
- Um eine Automatisierungsregel zu erstellen und ihr ein oder mehrere Tags hinzuzufügen, rufen Sie die [CreateAutomationRule](#)API auf oder führen Sie, falls Sie die verwenden AWS CLI, den [create-automation-rule](#)Befehl aus.
- Um Security Hub CSPM zu aktivieren und Ihrer Hub Ressource ein oder mehrere Tags hinzuzufügen, rufen Sie die [EnableSecurityHub](#)API auf oder führen Sie, falls Sie die AWS Command Line Interface (AWS CLI) verwenden, den Befehl aus. [enable-security-hub](#)

Verwenden Sie in Ihrer Anfrage den `tags` Parameter, um den Tag-Schlüssel und den optionalen Tag-Wert für jedes Tag anzugeben, das der Ressource hinzugefügt werden soll. Der `tags` Parameter gibt ein Array von Objekten an. Jedes Objekt gibt einen Tag-Schlüssel und den zugehörigen Tag-Wert an.

Um einer vorhandenen Ressource ein oder mehrere Tags hinzuzufügen, verwenden Sie den [TagResource](#) Betrieb der Security Hub CSPM-API oder, falls Sie den verwenden AWS CLI, führen Sie den Befehl [tag-resource](#) aus. Geben Sie in Ihrer Anfrage den Amazon-Ressourcennamen (ARN) der Ressource an, der Sie ein Tag hinzufügen möchten. Verwenden Sie den `tags` Parameter, um den Tag-Schlüssel (`key`) und den optionalen Tag-Wert (`value`) für jedes hinzuzufügende Tag anzugeben. Der `tags` Parameter gibt ein Array von Objekten an, ein Objekt für jeden Tag-Schlüssel und den zugehörigen Tag-Wert.

Der folgende AWS CLI Befehl fügt beispielsweise der angegebenen Konfigurationsrichtlinie einen Prod Tag-Schlüssel mit einem Tag-Wert hinzu. `Environment` Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (`\`) zur Verbesserung der Lesbarkeit.

Beispiel für einen CLI-Befehl:

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Environment":"Prod"}'
```

Wobei gilt:

- `resource-arn` gibt den ARN der Konfigurationsrichtlinie an, zu der ein Tag hinzugefügt werden soll.
- **`Environment`** ist der Tag-Schlüssel des Tags, das der Regel hinzugefügt werden soll.
- **`Prod`** ist der Tag-Wert für den angegebenen Tag-Schlüssel (**`Environment`**).

Im folgenden Beispiel fügt der Befehl der Konfigurationsrichtlinie mehrere Tags hinzu.

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Environment":"Prod", "CostCenter":"12345", "Owner":"jane-doe"}'
```

Für jedes Objekt in einem tags Array sind key sowohl die value Argumente als auch erforderlich. Der Wert für das value Argument kann jedoch eine leere Zeichenfolge sein. Wenn Sie einem Tag-Schlüssel keinen Tag-Wert zuordnen möchten, geben Sie keinen Wert für das value Argument an. Mit dem folgenden Befehl wird beispielsweise ein Owner Tag-Schlüssel ohne zugehörigen Tag-Wert hinzugefügt:

```
$ aws securityhub tag-resource \  
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/  
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \  
--tags '{"Owner":""}'
```

Wenn ein Tagging-Vorgang erfolgreich ist, gibt Security Hub CSPM eine leere HTTP 200-Antwort zurück. Andernfalls gibt Security Hub CSPM eine HTTP 4 xx - oder 500-Antwort zurück, die angibt, warum der Vorgang fehlgeschlagen ist.

Tags für Security Hub CSPM-Ressourcen bearbeiten

Wenn sich Ihre Umgebung oder Anforderungen im Laufe der Zeit ändern, können Sie bestehende Tags für Ihre AWS Security Hub Cloud Security Posture Management (CSPM) -Ressourcen auswerten und die Tags nach Bedarf ändern. Ein Tag ist eine Bezeichnung, die Sie definieren und einer oder mehreren AWS Ressourcen zuweisen, einschließlich bestimmter Typen von Macie-Ressourcen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Ein Tag-Schlüssel ist eine allgemeine Bezeichnung, die als Kategorie für einen spezifischeren Tag-Wert dient. Ein Tag-Wert dient als Bezeichnung für einen Tag-Schlüssel.

Mithilfe von Tags können Sie Ressourcen auf unterschiedliche Weise identifizieren, kategorisieren und verwalten, z. B. nach Zweck, Eigentümer, Umgebung oder anderen Kriterien. Sie können Tags beispielsweise verwenden, um Richtlinien anzuwenden, Kosten zuzuweisen, zwischen Versionen von Ressourcen zu unterscheiden oder Ressourcen zu identifizieren, die bestimmte Compliance-Anforderungen oder Workflows unterstützen.

Sie können Tags zu den folgenden Typen von Security Hub CSPM-Ressourcen hinzufügen:

- Regeln für die Automatisierung
- Konfigurationsrichtlinien
- Hub-Ressource

Um Tag-Schlüssel oder Tag-Werte für eine Security Hub CSPM-Ressource zu bearbeiten, können Sie die Security Hub CSPM-API verwenden. Die Security Hub CSPM-Konsole unterstützt derzeit keine Tag-Bearbeitung.

 Important

Das Bearbeiten von Tags für eine Ressource kann sich auf den Zugriff auf die Ressource auswirken. Bevor Sie ein Tag für eine Ressource bearbeiten, überprüfen Sie alle AWS Identity and Access Management (IAM-) Richtlinien, die möglicherweise Tags verwenden, um den Zugriff auf Ressourcen zu steuern.

Security Hub CSPM API

So bearbeiten Sie Tags für eine Security Hub CSPM-Ressource (API)

Wenn Sie ein Tag für eine Ressource programmgesteuert bearbeiten, überschreiben Sie das vorhandene Tag mit neuen Werten. Daher hängt die beste Methode zum Bearbeiten eines Tags davon ab, ob Sie einen Tag-Schlüssel, einen Tag-Wert oder beides bearbeiten möchten. Um einen Tag-Schlüssel zu bearbeiten, [entfernen Sie das aktuelle Tag](#) und [fügen Sie ein neues Tag](#) hinzu.

Um nur den Tag-Wert zu bearbeiten oder zu entfernen, der einem Tag-Schlüssel zugeordnet ist, überschreiben Sie den vorhandenen Wert mithilfe [TagResource](#) der Security Hub CSPM-API. [Wenn Sie den verwenden, führen Sie den Befehl AWS CLI tag-resource aus](#). Geben Sie in Ihrer Anfrage den Amazon-Ressourcennamen (ARN) der Ressource an, deren Tag-Wert Sie bearbeiten oder entfernen möchten.

Um einen Tag-Wert zu bearbeiten, verwenden Sie den tags Parameter, um den Tag-Schlüssel anzugeben, dessen Tag-Wert Sie ändern möchten. Sie sollten auch den neuen Tag-Wert für den Schlüssel angeben. Mit dem folgenden AWS CLI Befehl wird beispielsweise der Tag-Wert Test für Prod den Environment Tag-Schlüssel, der der angegebenen Automatisierungsregel zugewiesen ist, von auf geändert. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Environment":"Test"}'
```


Wobei gilt:

- `resource-arn` gibt den ARN der Konfigurationsrichtlinie an.
- `Environment` ist der Tag-Schlüssel, der dem zu ändernden Tag-Wert zugeordnet ist.
- `Test` ist der neue Tag-Wert für den angegebenen Tag-Schlüssel (`Environment`).

Um einen Tag-Wert aus einem Tag-Schlüssel zu entfernen, geben Sie im `tags` Parameter keinen Wert für das `value` Argument des Schlüssels an. Zum Beispiel:

```
$ aws securityhub tag-resource \  
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/  
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \  
--tags '{"Owner":""}'
```

Wenn der Vorgang erfolgreich ist, gibt Security Hub CSPM eine leere HTTP 200-Antwort zurück. Andernfalls gibt Security Hub CSPM eine HTTP 4 xx - oder 500-Antwort zurück, die angibt, warum der Vorgang fehlgeschlagen ist.

Tags für Security Hub CSPM-Ressourcen überprüfen

Nachdem Sie Tags für AWS Security Hub Cloud Security Posture Management (CSPM) -Ressourcen hinzugefügt oder bearbeitet haben, können Sie sehen, über welche Tag-Schlüssel und Tag-Werte eine Ressource derzeit verfügt. Ein Tag ist eine Bezeichnung, die Sie definieren und einer oder mehreren AWS Ressourcen zuweisen, einschließlich bestimmter Typen von Macie-Ressourcen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Ein Tag-Schlüssel ist eine allgemeine Bezeichnung, die als Kategorie für einen spezifischeren Tag-Wert dient. Ein Tag-Wert dient als Bezeichnung für einen Tag-Schlüssel.

Mithilfe von Tags können Sie Ressourcen auf unterschiedliche Weise identifizieren, kategorisieren und verwalten, z. B. nach Zweck, Eigentümer, Umgebung oder anderen Kriterien. Sie können Tags beispielsweise verwenden, um Richtlinien anzuwenden, Kosten zuzuweisen, zwischen Versionen von Ressourcen zu unterscheiden oder Ressourcen zu identifizieren, die bestimmte Compliance-Anforderungen oder Workflows unterstützen.

Sie können Tags zu den folgenden Typen von Security Hub CSPM-Ressourcen hinzufügen:

- Regeln für die Automatisierung

- Konfigurationsrichtlinien
- Hub-Ressource

Sie können die Tags für eine Security Hub CSPM-Automatisierungsregel oder eine Konfigurationsrichtlinie überprüfen, indem Sie die Security Hub CSPM-Konsole oder die Security Hub CSPM-API verwenden. Die Konsole unterstützt die Überprüfung von Tags für die Ressource nicht. Hub Programmgesteuert können Sie Tags für jede Ressource überprüfen.

[Verwenden Sie die Tagging-Operationen der Tagging-API, um Tags für mehrere Security Hub CSPM-Ressourcen gleichzeitig zu überprüfen.](#)[AWS Resource Groups](#)

Console

So überprüfen Sie Tags für eine Security Hub CSPM-Ressource (Konsole)

1. Öffnen Sie mit den Anmeldeinformationen des Security Hub CSPM-Administrators die AWS Security Hub Cloud Security Posture Management (CSPM) -Konsole unter. <https://console.aws.amazon.com/securityhub/>
2. Gehen Sie je nach Art der Ressource, der Sie ein Tag hinzufügen möchten, wie folgt vor:
 - Um die Tags für eine Automatisierungsregel zu überprüfen, wählen Sie im Navigationsbereich Automatisierungen aus. Wählen Sie dann eine Automatisierungsregel aus.
 - Um die Tags für eine Konfigurationsrichtlinie zu überprüfen, wählen Sie im Navigationsbereich Konfiguration aus. Wählen Sie dann auf der Registerkarte Richtlinien die Option neben einer Konfigurationsrichtlinie aus. Ein Seitenbereich wird geöffnet, in dem die Anzahl der der Richtlinie zugewiesenen Tags angezeigt wird. Sie können den Tags-Header erweitern, um die Tag-Schlüssel und Tag-Werte zu sehen.

Im Abschnitt „Tags“ werden alle Tags aufgeführt, die der Ressource derzeit zugewiesen sind.

Security Hub CSPM API

Um Tags für eine Security Hub CSPM-Ressource (API) zu überprüfen

Rufen Sie die API auf, um die Tags für eine bestehende Ressource abzurufen und zu überprüfen. [ListTagsForResource](#) Verwenden Sie in Ihrer Anfrage den `resourceArn` Parameter, um den Amazon-Ressourcennamen (ARN) der Ressource anzugeben.

Wenn Sie den verwenden AWS CLI, führen Sie den [list-tags-for-resource](#) Befehl aus und geben Sie mit dem `resource-arn` Parameter den ARN der Ressource an. Zum Beispiel:

```
$ aws securityhub list-tags-for-resource --resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Wenn der Vorgang erfolgreich ist, gibt Security Hub CSPM ein Array zurück. tags Jedes Objekt im Array spezifiziert ein Tag (sowohl den Tag-Schlüssel als auch den Tag-Wert), das der Ressource aktuell zugewiesen ist. Zum Beispiel:

```
{
  "tags": [
    {
      "key": "Environment",
      "value": "Prod"
    },
    {
      "key": "CostCenter",
      "value": "12345"
    },
    {
      "key": "Owner",
      "value": ""
    }
  ]
}
```

Wobei `Environment`, `CostCenter`, und `Owner` die Tag-Schlüssel sind, die der Ressource zugewiesen sind. `Prod` ist der Tag-Wert, der dem `Environment` Tag-Schlüssel zugeordnet ist. `12345` ist der Tag-Wert, der dem `CostCenter` Tag-Schlüssel zugeordnet ist. Dem `Owner` Tag-Schlüssel ist kein Tag-Wert zugeordnet.

Um eine Liste aller Security Hub CSPM-Ressourcen mit Tags und aller Tags, die jeder dieser Ressourcen zugewiesen sind, abzurufen, verwenden Sie den [GetResources](#) Betrieb der AWS Resource Groups Tagging-API. Setzen Sie in Ihrer Anfrage den Wert für den Parameter `resourceTypeFilters` auf `securityhub`. Führen Sie dazu mit dem den AWS CLI Befehl [get-resources](#) aus und setzen Sie den Wert für den `resource-type-filters` Parameter auf `securityhub`. Zum Beispiel:

```
$ aws resourcegroupstaggingapi get-resources --resource-type-filters "securityhub"
```

Wenn der Vorgang erfolgreich ist, gibt Resource Groups ein `ResourceTagMappingList` Array zurück. Das Array enthält ein Objekt für jede Security Hub-CSPM-Ressource, die über Tags verfügt. Jedes Objekt spezifiziert den ARN einer Security Hub-CSPM-Ressource sowie die Tag-Schlüssel und -Werte, die der Ressource zugewiesen sind.

Tags aus den CSPM-Ressourcen von Security Hub entfernen

Wenn Sie einer AWS Security Hub Cloud Security Posture Management (CSPM) -Ressource Tags hinzufügen, können Sie anschließend eines oder mehrere davon entfernen. Ein Tag ist eine Bezeichnung, die Sie definieren und AWS Ressourcen zuweisen, einschließlich bestimmter Typen von Security Hub CSPM-Ressourcen. Sie können Tags zu den folgenden Typen von Security Hub CSPM-Ressourcen hinzufügen, bearbeiten und entfernen: Automatisierungsregeln, Konfigurationsrichtlinien und die Hub Ressource.

Um Tags aus einer einzelnen AWS Security Hub Cloud Security Posture Management (CSPM) -Ressource zu entfernen, können Sie die Security Hub CSPM-API verwenden. Die Security Hub CSPM-Konsole unterstützt derzeit das Entfernen von Tags nicht.

[Um Tags aus mehreren Security Hub CSPM-Ressourcen gleichzeitig zu entfernen, verwenden Sie die Tagging-Operationen der AWS Resource Groups Tagging-API.](#)

Important

Das Entfernen von Tags aus einer Ressource kann sich auf den Zugriff auf die Ressource auswirken. Bevor Sie ein Tag entfernen, überprüfen Sie alle AWS Identity and Access Management (IAM-) Richtlinien, die das Tag möglicherweise zur Steuerung des Zugriffs auf Ressourcen verwenden.

Security Hub CSPM API

So entfernen Sie Tags aus einer Security Hub CSPM-Ressource (API)

Um ein oder mehrere Tags programmgesteuert aus einer Ressource zu entfernen, verwenden Sie den [UntagResource](#) Betrieb der Security Hub CSPM-API. Verwenden Sie in Ihrer Anfrage den `resourceArn` Parameter, um den Amazon-Ressourcennamen (ARN) der Ressource anzugeben, aus der ein Tag entfernt werden soll. Verwenden Sie den `tagKeys` Parameter, um den Tag-Schlüssel des Tags anzugeben, das entfernt werden soll. Um mehrere Tags zu entfernen, hängen

Sie den `tagKeys` Parameter und das Argument für jedes zu entfernende Tag an, getrennt durch ein Und-Zeichen (&) — zum Beispiel. `tagKeys=key1&tagKeys=key2` Um nur einen bestimmten Tag-Wert (keinen Tag-Schlüssel) aus einer Ressource zu entfernen, [bearbeiten Sie das Tag, anstatt das Tag](#) zu entfernen.

Wenn Sie den verwenden AWS CLI, führen Sie den Befehl [untag-resource](#) aus, um ein oder mehrere Tags aus einer Ressource zu entfernen. Geben Sie für den `resource-arn` Parameter den ARN der Ressource an, aus der ein Tag entfernt werden soll. Verwenden Sie den `tag-keys` Parameter, um den Tag-Schlüssel des Tags anzugeben, das entfernt werden soll. Mit dem folgenden Befehl wird beispielsweise das Environment Tag (sowohl der Tag-Schlüssel als auch der Tag-Wert) aus der angegebenen Konfigurationsrichtlinie entfernt:

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment
```

Where `resource-arn` gibt den ARN der Konfigurationsrichtlinie an, aus der ein Tag entfernt werden soll, und `Environment` ist der Tag-Schlüssel des zu entfernenden Tags.

Um mehrere Tags aus einer Ressource zu entfernen, fügen Sie jeden zusätzlichen Tag-Schlüssel als Argument für den `tag-keys` Parameter hinzu. Zum Beispiel:

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment Owner
```

Wenn der Vorgang erfolgreich ist, gibt Security Hub CSPM eine leere HTTP 200-Antwort zurück. Andernfalls gibt Security Hub CSPM eine HTTP 4 xx - oder 500-Antwort zurück, die angibt, warum der Vorgang fehlgeschlagen ist.

Kontingente für Security Hub CSPM

Für jedes Ihrer AWS-Konto Kontingente gelten bestimmte Standardkontingente, die früher als Limits bezeichnet wurden. AWS-Service Diese Kontingente sind die maximale Anzahl von Serviceressourcen oder Vorgängen für Ihr Konto. Dieses Thema enthält Links zu den Kontingenten, die für die Ressourcen und Operationen von AWS Security Hub Cloud Security Posture Management (CSPM) für Ihr Konto gelten. Sofern nicht anders angegeben, gilt jedes Kontingent jeweils für Ihr Konto. AWS-Region

Einige Kontingente können erhöht werden, andere dagegen nicht. Verwenden Sie die [Service Quotas-Konsole, um eine Erhöhung eines Kontingents](#) anzufordern. Informationen dazu, wie Sie eine Erhöhung beantragen können, finden Sie unter [Eine Erhöhung des Kontingents beantragen](#) im Benutzerhandbuch zu Service Quotas. Wenn ein Kontingent in der Service-Kontingents-Konsole nicht verfügbar ist, verwenden Sie das [Formular zur Erhöhung des Servicelimits](#) auf der AWS Support Center Console , um eine Erhöhung des Kontingents zu beantragen.

Maximale Kontingente

Eine Liste der Kontingente, die für Security Hub CSPM-Ressourcen gelten, finden Sie unter [AWS Security Hub Cloud Security Posture Management \(CSPM\) -Endpunkte](#) und Kontingente in der. Allgemeine AWS-Referenz

Ratenkontingente

Eine Liste der Kontingente, die für Security Hub CSPM-API-Operationen gelten, finden Sie in der [AWS Security Hub Cloud Security Posture Management \(CSPM\)](#) API-Referenz.

Wenn Sie die [regionsübergreifende Aggregation in Security Hub CSPM](#) einrichten, erfolgt ein einziger Aufruf BatchImportFindings und BatchUpdateFindings wirkt sich auf verknüpfte Regionen und die Aggregationsregion aus. Der GetFindings Vorgang ruft Ergebnisse aus verknüpften Regionen und der Aggregationsregion ab. Die UpdateStandardsControl Operationen BatchEnableStandards und sind jedoch regionsspezifisch.

Dokumentenverlauf für das AWS Security Hub Hub-Benutzerhandbuch

In der folgenden Tabelle werden die wichtigen Änderungen an der Dokumentation seit der letzten Version von AWS Security Hub und Security Hub CSPM beschrieben. Bei Versionen neuer CSPM-Sicherheitskontrollen gibt das Datum an, ab wann die Kontrollen im unterstützten Bereich verfügbar sind. AWS-Regionen Es kann 1-2 Wochen dauern, bis die Kontrollen in allen unterstützten Regionen verfügbar sind.

Um über Aktualisierungen des AWS Security Hub Hub-Benutzerhandbuchs informiert zu werden, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Regionale Verfügbarkeit	Security Hub CSPM ist jetzt in der Region Asien-Pazifik (Taipeh) verfügbar. Eine vollständige Liste, AWS-Regionen wo Security Hub CSPM derzeit verfügbar ist, finden Sie unter AWS Security Hub Hub-Endpunkte und Kontingente in der. Allgemeine AWS-Referenz	23. Juli 2025
Neue Integration von Drittanbietern	Dynatrace ist eine neue Drittanbieter-Integration , die Erkenntnisse von Security Hub CSPM erhalten kann.	18. Juli 2025
Neue Sicherheitskontrollen	Security Hub CSPM hat 13 neue Kontrollen veröffentlicht. Die meisten Kontrollen unterstützen den FSBP-Standard (AWS Foundational Security Best Practices)	15. Juli 2025

). Einige der Steuerungen unterstützen die Anforderungen von [NIST SP 800-53 Rev. 5](#).

- [Für den AWS FSBP-Standard gelten folgende Kontrollen: CloudFront.15, IDs Cognito.2, EC2 .180, ELB.18, MSK.4, MSK.5, MSK.6, RDS.45, Redshift.18, S3.25, SSM.6 und SSM.7.](#)
- [Für NIST SP 800-53 Rev. 5 gelten folgende Steuerungen: Lambda.7 und RDS.45. IDs](#)

[Aktualisierungen zur Generierung von Kontrollberufen](#)

Um Ihnen die Nachverfolgung von Compliance-Änderungen zu erleichtern, [aktualisiert Security Hub CSPM jetzt bestehende Kontrollergebnisse](#), anstatt neue Ergebnisse zu generieren, wenn sich der Compliance-Status einzelner Ressourcen ändert. Das bedeutet, dass Sie anhand der Daten einzelner Ergebnisse die Compliance-Änderungen für bestimmte Ressourcen anhand bestimmter Kontrollen verfolgen können.

3. Juli 2025

Aktualisierungen der Sicherheitsstandards und -kontrollen

Wir haben die [IAM.13-Steuerung](#) aus dem [PCI DSS v4.0.1-Standard](#) entfernt. [Wir haben auch das IAM.17-Steurelement aus dem Standard NIST SP 800-171 Revision 2 entfernt.](#) Die Standards schreiben die Prüfungen, die diese Kontrollen bieten, nicht ausdrücklich vor. Wir haben auch die zugehörigen Anforderungsdetails für diese Standards für bestimmte Kontrollen aktualisiert, die IAM-Passwortrichtlinien überprüfen: IAM.7 und IAM.10 bis IAM.17.

30. Juni 2025

Aktualisierungen bei Finding Retention

Security Hub CSPM [speichert archivierte Ergebnisse](#) jetzt für 30 Tage statt für 90 Tage, wodurch die Anzahl der Ergebnisse reduziert werden kann. Für eine längerfristige Aufbewahrung können Sie Ergebnisse in einen S3-Bucket exportieren, indem Sie [eine benutzerdefinierte Aktion mit einer EventBridge Amazon-Regel verwenden](#).

20. Juni 2025

Aktualisierungen vorhandener verwalteter Richtlinien

Security Hub CSPM hat der [AWS verwalteten Richtlinie](#) mit dem Namen eine neue Berechtigung hinzugefügt. `AWSecurityHubOrganizationsAccess` Die Berechtigung ermöglicht es der Unternehmensleitung, Security Hub und Security Hub CSPM innerhalb einer Organisation zu aktivieren und zu verwalten. Security Hub CSPM fügte der AWS verwalteten Richtlinie mit dem Namen auch eine neue Berechtigung hinzu. `AWSecurityHubFullAccess` Die Berechtigung ermöglicht es Principals, eine dienstbezogene Rolle für Security Hub zu erstellen.

18. Juni 2025

Öffentliche Vorschauversion und eine neue verwaltete Richtlinie für Security Hub

Öffentliche Vorschauversion von AWS Security Hub und das [AWS Security Hub Hub-Benutzerhandbuch](#). Diese Version enthält eine neue [AWS verwaltete Richtlinie](#), `AWSecurityHubV2ServiceRolePolicy`. Die Richtlinie ermöglicht es Security Hub, AWS Config Regeln und Security Hub Hub-Ressourcen in der Organisation eines Kunden und im Namen des Kunden zu verwalten. Security Hub befindet sich in der Vorschauversion und kann sich ändern.

17. Juni 2025

Aktualisierungen der Sicherheitsstandards und -kontrollen

Wir haben die [IAM.10-Steuerung](#) aus dem [PCI DSS v4.0.1-Standard](#) entfernt. Dieses Steuerelement prüft, ob die Kontopasswortrichtlinien für IAM-Benutzer die Mindestanforderungen erfüllen, einschließlich einer Mindestkennwortlänge von 7 Zeichen. PCI DSS v4.0.1 verlangt jetzt, dass Passwörter mindestens 8 Zeichen lang sind. Die IAM.10-Steuerung gilt weiterhin für den Standard PCI DSS v3.2.1, für den andere Kennwortanforderungen gelten.

30. Mai 2025

Neuer Sicherheitsstandard

Security Hub CSPM bietet jetzt einen [Sicherheitsstandard](#), der dem Cybersicherheits- und Compliance-Framework von NIST SP 800-171 Revision 2 entspricht. Dieser neue Standard umfasst mehr als 60 bestehende Sicherheitskontrollen. Die Kontrollen führen automatisierte Prüfungen durch, bei denen bestimmte AWS-Services Ressourcen im Hinblick auf die Einhaltung einer Teilmenge der im Framework definierten Anforderungen bewertet werden.

29. Mai 2025

Aktualisierungen der Sicherheitskontrollen

Security Hub CSPM hat die Veröffentlichung der folgenden Steuerung insgesamt rückgängig gemacht AWS-Regionen: [RDS.46] RDS-DB-Instances sollten nicht in öffentlichen Subnetzen mit Routen zu Internet-Gateways bereitgestellt werden. Bisher unterstützte dieses Steuerelement den FSBP-Standard (AWS Foundational Security Best Practices).

8. Mai 2025

Neue Sicherheitskontrollen

7. Mai 2025

Security Hub CSPM hat 9 neue Kontrollen veröffentlicht. Die meisten Kontrollen unterstützen den [FSBP-Standard \(AWS Foundational Security Best Practices\)](#). Einige der Steuerungen unterstützen die Anforderungen von [NIST SP 800-53 Rev. 5](#).

- [Für den AWS FSBP-Standard gelten folgende Steuerelemente:](#)
[DocumentDB.6](#), [RDS.44](#),
[RedshiftServerless.2](#),
[RedshiftServerless.3](#), [.5](#), [.6](#)
[und RedshiftServerless](#)
[.7. IDs RedshiftServerless](#)
[RedshiftServerless](#)
- [Für NIST SP 800-53 Rev. 5 gelten folgende Steuerungen:](#) [.10](#), [.4](#) und
[IDs .7. CloudTrail RedshiftServerless RedshiftServerless](#)

Neue Sicherheitskontrollen

Security Hub CSPM hat 24 neue Kontrollen veröffentlicht. Die meisten Kontrollen unterstützen den Standard AWS Foundational Security Best Practices (FSBP) oder AWS Resource Tagging.

Einige der Kontrollen unterstützen die Anforderungen von NIST SP 800-53 Rev. 5.

16. April 2025

- Für den AWS FSBP-Standard gelten folgende Kontrollen: EC2.173, IDs RDS.41, RDS.42 und .8. SageMaker
- Für den AWS Resource Tagging-Standard gelten folgende Steuerelemente: Amplify.1, IDs Amplify.2, Batch.4, DataSync.2, EC2 .174, EC2 .175, EC2 .176, EC2 .177, EC2 .178, .179, Redshift.17, .6, .7, SSM.5, Transfer.4, EC2Transfer.5, SageMaker SageMaker <https://docs.aws.amazon.com/securityhub/latest/userguide/transfer-controls.html#transfer-6Transfer.6 und Transfer.7.>
- Für NIST SP 800-53 Rev. 5 gelten IDs für die entsprechenden Kontrollen: ECS.17 und RDS.42.

Neue Sicherheitskontrollen

18. März 2025

Security Hub CSPM hat vier neue Kontrollen für den Standard [AWS Foundational Security Best Practices](#) veröffentlicht. Die Kontrollen sind:

- [the section called “\[FSx.3\] FSx für OpenZFS-Dateisysteme sollte für die Multi-AZ-Bereitstellung konfiguriert werden”](#)
- [the section called “\[FSx.4\] FSx für NetApp ONTAP-Dateisysteme sollte für die Multi-AZ-Bereitstellung konfiguriert sein”](#)
- [the section called “\[FSx.5\] FSx für Windows-Dateiserver sollten für die Multi-AZ-Bereitstellung konfiguriert sein”](#)
- [the section called “\[RedshiftServerless.1\] Serverlose Amazon Redshift Redshift-Arbeitsgruppen sollten erweitertes VPC-Routing verwenden”](#)

Aktualisierungen der Sicherheitsstandards und -kontrollen

Wir haben die [Sicherheitsskontrolle RDS.18](#) aus dem Standard „Best Practices“ AWS von Foundation Security entfernt und die Überprüfung der Anforderungen von NIST SP 800-53 Rev. 5 automatisiert. Da Amazon EC2 -Classic Networking eingestellt wurde, können Amazon Relational Database Service (Amazon RDS) -Instances nicht mehr außerhalb einer VPC bereitgestellt werden. [Die Steuerung ist weiterhin Teil des Service-Managed-Standards.AWS Control Tower](#)

7. März 2025

Aktualisierungen der Kontrolleergebnisse

Security Hub CSPM generiert jetzt WARNING Ergebnisse für ein aktiviertes Steuerelement, wenn die [Ressourcenaufzeichnung](#) AWS Config für den Ressourcentyp, den das Steuerelement überprüft, nicht aktiviert ist. Dies kann Ihnen helfen, potenzielle Konfigurationslücken bei Ihren Sicherheitskontrollen zu identifizieren und zu beheben.

25. Februar 2025

Neue Sicherheitskontrollen

Security Hub CSPM hat 11 neue Kontrollen veröffentlicht. Die Kontrollen sind:

24. Februar 2025

- [the section called “\[Connect .2\] Für Amazon Connect Connect-Instances sollte die Protokollierung aktiviert sein CloudWatch ”](#)
- [the section called “\[ECR.5\] ECR-Repositorys sollten verschlüsselt und vom Kunden verwaltet werden AWS KMS keys”](#)
- [the section called “\[ELB.17\] Anwendungs- und Netzwerk-Load-Balancer mit Listnern sollten die empfohlenen Sicherheitsrichtlinien verwenden”](#)
- [the section called “\[Glue.4\] AWS Glue Spark-Jobs sollten auf unterstützten Versionen von ausgeführt werden AWS Glue”](#)
- [the section called “\[GuardDuty.11\] GuardDuty Runtime Monitoring sollte aktiviert sein”](#)
- [the section called “\[GuardDuty.12\] GuardDuty ECS Runtime Monitoring sollte aktiviert sein”](#)
- [the section called “\[GuardDuty.13\] GuardDuty EC2](#)

Runtime Monitoring sollte aktiviert sein”

- the section called “[Network Firewall.10] Bei Netzwerk-Firewall-Firewalls sollte der Subnetzänderungsschutz aktiviert sein”
- the section called “[RDS.40] RDS für SQL Server-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch ”
- the section called “[SQS.3] Die Richtlinien für den Zugriff auf SQS-Warteschlangen sollten keinen öffentlichen Zugriff zulassen”
- the section called “[Transfer.3] Bei Connectoren der Transfer-Familie sollte die Protokollierung aktiviert sein”

Neue Sicherheitskontrollen

Security Hub CSPM hat 37 neue Steuerelemente für den [AWS Resource Tagging](#) Standard veröffentlicht. Security Hub CSPM hat außerdem die folgenden neuen Steuerelemente veröffentlicht:

22. Januar 2025

- [the section called “\[EMR.3\] Amazon EMR-Sicherheitskonfigurationen sollten im Ruhezustand verschlüsselt werden”](#)
- [the section called “\[EMR.4\] Amazon EMR-Sicherheitskonfigurationen sollten bei der Übertragung verschlüsselt werden”](#)
- [the section called “\[SageMaker.5\] SageMaker Modelle sollten eingehenden Datenverkehr blockieren”](#)

Neue Sicherheitskontrolle

Security Hub CSPM veröffentlichte Version [EC21.72 Die EC2 VPC-Einstellungen für Block Public Access sollten den Internet-Gateway-Verkehr blockieren](#).

15. Januar 2025

Neue Sicherheitskontrollen

Die folgenden neuen Security Hub CSPM-Steurelemente sind verfügbar.

17. Dezember 2024

- [the section called “\[Cognito.1\] In Cognito-Benutzerpools sollte der Bedrohungsschutz mit vollem Funktionsumfang für die Standardauthentifizierung aktiviert sein”](#)
- [the section called “\[RDS.38\] RDS für PostgreSQL-DB-Instances sollten bei der Übertragung verschlüsselt werden”](#)
- [the section called “\[RDS.39\] RDS für MySQL-DB-Instances sollten bei der Übertragung verschlüsselt werden”](#)
- [the section called “\[Redshift.16\] Redshift-Cluster-Subnetzgruppen sollten Subnetze aus mehreren Availability Zones haben”](#)

Security Hub CSPM unterstützt PCI DSS v4.0.1

Security Hub CSPM unterstützt jetzt Version 4.0.1 des Payment Card Industry Data Security Standard (PCI DSS). Weitere Informationen zum Standard und den dafür geltenden Kontrollen finden Sie unter [PCI DSS in Security Hub CSPM](#).

11. Dezember 2024

[Security Hub CSPM erhält Ergebnisse zur GuardDuty Angriffssequenz](#)

Security Hub CSPM erhält jetzt Ergebnisse zur Angriffssequenz von Amazon GuardDuty Extended Threat Detection. Einzelheiten zum Auffinden der Angriffssequenz sind im [Erkennungsobjekt](#) des AWS Security Finding Formats (ASFF) verfügbar.

01. Dezember 2024

[Security Hub CSPM wird ab sofort unterstützt AWS-Region](#)

Security Hub CSPM ist jetzt in der Region Asien-Pazifik (Malaysia) verfügbar. Für einige Sicherheitskontrollen gelten regionale Einschränkungen. Eine Liste der Kontrollen, die in dieser Region nicht verfügbar sind, finden Sie unter [Regionale Beschränkungen für Security Hub CSPM-Steuerelemente](#).

22. November 2024

[Änderungen an Config.1](#)

Security Hub CSPM erhöhte den Schweregrad des Config.1-Steuerelements von MEDIUM bis CRITICAL und fügte neue Statuscodes und Statusgründe für fehlgeschlagene Config.1-Ergebnisse hinzu. Weitere Informationen zu den Änderungen finden Sie im Eintrag vom 20. November 2024 im [Änderungsprotokoll für Security Hub CSPM-Steuerelemente](#).

20. November 2024

Neue Sicherheitskontrollen

15. November 2024

Die folgenden neuen Security Hub CSPM-Steuerelemente sind verfügbar. Diese Kontrollen sind Teil von AWS Foundational Security Best Practices und NIST SP 800-53 Rev. 5 und bewerten, ob eine von Ihnen verwaltete Virtual Private Cloud (VPC) über einen Schnittstellen-VPC-Endpoint für eine OR-Ressource verfügt. AWS-Service AWS

- [the section called “\[EC2.55\] VPCs sollte mit einem Schnittstellenendpoint für die ECR-API konfiguriert werden”](#)
- [the section called “\[EC2.56\] VPCs sollte mit einem Schnittstellenendpoint für Docker Registry konfiguriert werden”](#)
- [the section called “\[EC2.57\] VPCs sollte mit einem Schnittstellenendpoint für Systems Manager konfiguriert werden”](#)
- [the section called “\[EC2.58\] VPCs sollte mit einem Schnittstellenendpoint für Systems Manager Incident Manager-Kontakte konfiguriert sein”](#)

- [the section called “\[EC2.60\] VPCs sollte mit einem Schnittstellenendpunkt für Systems Manager Incident Manager konfiguriert werden”](#)

Neue Sicherheitskontrollen

Die folgenden neuen Security Hub CSPM-Steuerelemente sind verfügbar.

18. Oktober 2024

- the section called “[AppSync .1] AWS AppSync API-Caches sollten im Ruhezustand verschlüsselt werden”
- the section called “[AppSync .6] AWS AppSync API-Caches sollten bei der Übertragung verschlüsselt werden”
- the section called “[EC2.170] EC2 Startvorlagen sollten Instance Metadata Service Version 2 () verwenden IMDSv2”
- the section called “[EC2.171] Bei EC2 VPN-Verbindungen sollte die Protokollierung aktiviert sein”
- the section called “[EFS.8] EFS-Dateisysteme sollten im Ruhezustand verschlüsselt werden”
- the section called “[KMS.5] KMS-Schlüssel sollten nicht öffentlich zugänglich sein”
- the section called “[SNS.4] Zugriffsrichtlinien für SNS-Themen sollten keinen öffentlichen Zugriff zulassen”

Neue Sicherheitskontrollen

Die folgenden neuen Security Hub CSPM-Steuerelemente sind verfügbar.

3. Oktober 2024

- the section called “[ECS.16] ECS-Aufgabensätze sollten öffentliche IP-Adressen nicht automatisch zuweisen”
- the section called “[GuardDuty.7] GuardDuty EKS Runtime Monitoring sollte aktiviert sein”
- the section called “[Kinesis.3] Kinesis-Streams sollten über eine angemessene Aufbewahrungsfrist für Daten verfügen”
- the section called “[MSK.3] MSK Connect-Anschlüsse sollten bei der Übertragung verschlüsselt werden”
- the section called “[RDS.36] RDS für PostgreSQL-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch ”
- the section called “[RDS.37] Aurora PostgreSQL-DB-Cluster sollten Protokolle in Logs veröffentlichen CloudWatch ”
- the section called “[S3.24] Für S3-Access Points mit mehreren Regionen sollten die Einstellungen für die

Blockierung des öffentlichen
Zugriffs aktiviert sein”

Neue Sicherheitskontrollen

Die folgenden neuen Security Hub CSPM-Steurelemente sind verfügbar.

30. August 2024

- [the section called “\[Athena.4\] Bei Athena-Arbeitsgruppen sollte die Protokollierung aktiviert sein”](#)
- [the section called “\[CodeBuild.7\] Exporte von CodeBuild Berichtsgruppen sollten im Ruhezustand verschlüsselt werden”](#)
- [the section called “\[DataSync.c.1\] Für DataSync Aufgaben sollte die Protokollierung aktiviert sein”](#)
- [the section called “\[EFS.7\] Bei EFS-Dateisystemen sollten automatische Backups aktiviert sein”](#)
- Glue.2 (im Ruhezustand)
- [the section called “\[Glue.3\] Transformationen für AWS Glue maschinelles Lernen sollten im Ruhezustand verschlüsselt werden”](#)
- [the section called “\[WorkSpaces.1\] WorkSpaces Benutzervolumes sollten im Ruhezustand verschlüsselt werden”](#)
- [the section called “\[WorkSpaces.2\] WorkSpaces Root-Volumes sollten im](#)

Ruhezustand verschlüsselt werden"

Neues Findungspanel

Das [neue Ergebnisfenster](#) auf der Security Hub CSPM-Konsole hilft Ihnen, schnell Maßnahmen zu ergreifen, Ressourcendetails und den Befundverlauf zu überprüfen und weitere relevante Informationen zu einem Ergebnis zu finden.

16. August 2024

Update zur Config.1-Steuerung

Das [Config.1-Steuerelement](#) prüft, ob AWS Config es aktiviert ist, verwendet die dienstverknüpfte Rolle und zeichnet Ressourcen für aktivierte Steuerelemente auf. Security Hub CSPM hat einen benutzerdefinierten Steuerparameter mit dem Namen hinzugefügt. `includeConfigServiceLinkedRoleCheck` Wenn Sie diesen Parameter auf `setzenfalse`, können Sie sich von der Überprüfung abmelden, ob die serviceverknüpfte AWS Config Rolle verwendet wird.

15. August 2024

Geben Sie eine Heimatregion ohne verknüpfte Regionen an

Sie können jetzt einen Suchaggregator erstellen und eine Heimatregion einrichten, ohne eine Region mit der Heimatregion AWS-Regionen zu verknüpfen. Auf diese Weise können Sie die [zentrale Konfiguration](#) aktivieren, ohne verknüpfte Regionen angeben zu müssen.

25. Juli 2024

Wählen Sie Steuerelemente aus, die in mehreren Regionen verfügbar sind

Die folgenden Steuerelemente sind jetzt zusätzlich verfügbar AWS-Regionen, darunter USA Ost (Nord-Virginia) und USA Ost (Ohio).

15. Juli 2024

- the section called “[DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden”
- the section called “[DMS.10] Bei DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein”
- the section called “[DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein”
- the section called “[DMS.12] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein”
- the section called “[DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden”
- the section called “[EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden”
- the section called “[EKS.3] EKS-Cluster sollten

- verschlüsselte Kubernetes-Geheimnisse verwenden
- the section called “[FSx.2] FSx für Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden”
- the section called “[MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch”
- the section called “[MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein”
- the section called “[Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben”
- the section called “[Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen”
- the section called “[SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein”
- the section called “[ServiceCatalog.1] Servicekatalog

atalog-Portfolios sollten
nur innerhalb einer AWS
Organisation gemeinsam
genutzt werden”

- the section called “[Transfe
r.2] Transfer Family Family-
Server sollten kein FTP-
Protokoll für die Endpunktv
erbindung verwenden”

Neue Sicherheitskontrollen

Die folgenden neuen Security Hub CSPM-Steuererelemente sind verfügbar:

11. Juli 2024

- the section called “[GuardDuty.5] GuardDuty EKS Audit Log Monitoring sollte aktiviert sein”
- the section called “[GuardDuty.6] GuardDuty Lambda Protection sollte aktiviert sein”
- the section called “[GuardDuty.8] Der GuardDuty Malware-Schutz für EC2 sollte aktiviert sein”
- the section called “[GuardDuty.9] Der GuardDuty RDS-Schutz sollte aktiviert sein”
- the section called “[GuardDuty.10] Der GuardDuty S3-Schutz sollte aktiviert sein”
- the section called “[Inspector.1] Das EC2 Scannen mit Amazon Inspector sollte aktiviert sein”
- the section called “[Inspector.2] Das Amazon Inspector ECR-Scannen sollte aktiviert sein”
- the section called “[Inspector.3] Das Scannen von Amazon Inspector Lambda-Code sollte aktiviert sein”

- [the section called “\[Inspect or.4\] Das Standardscannen von Amazon Inspector Lambda sollte aktiviert sein”](#)

Veröffentlichung von CIS AWS Foundations Benchmark v3.0.0

Security Hub CSPM hat den [Center for Internet Security \(CIS\) AWS Foundations Benchmark](#) v3.0.0 veröffentlicht. Die Version enthält die folgenden neuen Steuerelemente sowie Zuordnungen zu mehreren vorhandenen Steuerelementen.

13. Mai 2024

- [the section called “\[EC2.53\] EC2 Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 zu Remote-Serververwaltungsports zulassen”](#)
- [the section called “\[EC2.54\] EC2 Sicherheitsgruppen sollten keinen Zugriff von: :/0 zu Remote-Serveradministrationsports zulassen”](#)
- [the section called “\[IAM.26\] Abgelaufene SSL/TLS Zertifikate, die in IAM verwaltet werden, sollten entfernt werden”](#)
- [the section called “\[IAM.27\] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWS Cloud Shell Full Access ”](#)
- [the section called “\[IAM.28\] Der externe Zugriffsanalysator für IAM Access Analyzer sollte aktiviert sein”](#)

- [the section called “\[S3.22\] S3-Allzweck-Buckets sollten Schreibereignisse auf Objektebene protokollieren”](#)
- [the section called “\[S3.23\] S3-Allzweck-Buckets sollten Leseereignisse auf Objektebene protokollieren”](#)

Neue Sicherheitskontrollen

Die folgenden neuen Security Hub CSPM-Steuerelemente sind verfügbar:

3. Mai 2024

- the section called “[DataFirehose.1] Firehose-Lieferströme sollten im Ruhezustand verschlüsselt werden”
- the section called “[DMS.10] Bei DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein”
- the section called “[DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein”
- the section called “[DMS.12] Auf DMS-Endpunkten für Redis OSS sollte TLS aktiviert sein”
- the section called “[DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden”
- the section called “[EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden”
- the section called “[EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden”

- the section called “[FSx.2] FSx für Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden”
- the section called “[MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch”
- the section called “[MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein”
- the section called “[Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben”
- the section called “[Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen”
- the section called “[SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein”
- the section called “[ServiceCatalog.1] Servicecatalog-Portfolios sollten nur innerhalb einer AWS

[Organisation gemeinsam genutzt werden”](#)

- [the section called “\[Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden”](#)

[AWS Standard für Ressourcen-Tagging](#)

Der [AWS Resource Tagging Standard](#) von Security Hub CSPM ist jetzt allgemein verfügbar, zusammen mit neuen Kontrollen, die für den Standard gelten.

30. April 2024

[Aktualisierung der bestehenden verwalteten Richtlinie](#)

Security Hub CSPM hat die [AWS verwaltete Richtlinie](#) mit dem Namen aktualisiert `AmazonSecurityHubFullAccess`, um Preisdetails für AWS-Services und Produkte abzurufen.

24. April 2024

[Kontextabhängige Konfiguration der Steuerparameter](#)

Wenn Sie die zentrale Konfiguration verwenden, können Sie [Steuerparameter jetzt kontextbezogen](#) auf der Detailseite eines Steuerelements auf der Security Hub CSPM-Konsole konfigurieren.

29. März 2024

[Aktualisierung der bestehenden verwalteten Richtlinie](#)

Security Hub CSPM hat die [AWS verwaltete Richtlinie](#) aktualisiert, `AWSecurityHubReadOnlyAccess` indem sie ein Feld hinzugefügt hat `Sid`.

22. Februar 2024

Neue Sicherheitskontrolle

Das Steuerelement [\[Macie.2\]](#) [Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein, ist jetzt verfügbar](#). Informationen zu regionalen Beschränkungen für dieses Steuerelement finden Sie unter [Verfügbarkeit von Steuerelementen nach Regionen](#).

19. Februar 2024

Security Hub CSPM in Kanada West (Calgary) verfügbar

Security Hub CSPM ist jetzt in Kanada West (Calgary) verfügbar. Alle Security Hub CSPM-Funktionen sind jetzt in dieser Region verfügbar , mit Ausnahme bestimmter Sicherheitskontrollen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

20. Dezember 2023

Neue Sicherheitskontrollen

Die folgenden neuen Security Hub CSPM-Steurelemente sind verfügbar:

14. Dezember 2023

- the section called “[Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein”
- the section called “[DynamoDB.6] Bei DynamoDB-Tabellen sollte der Löschschutz aktiviert sein”
- the section called “[EC2.51] EC2 Client-VPN-Endpunkte sollten die Client-Verbindungsprotokollierung aktiviert haben”
- the section called “[EKS.8] Bei EKS-Clustern sollte die Auditprotokollierung aktiviert sein”
- the section called “[EMR.2] Die Amazon EMR-Einstellung zum Blockieren des öffentlichen Zugriffs sollte aktiviert sein”
- the section called “[FSx.1] FSx für OpenZFS-Datensysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden”

- [the section called “\[Macie.1\] Amazon Macie sollte aktiviert sein”](#)
- [the section called “\[MSK.2\] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein”](#)
- [the section called “\[Neptune .9\] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden”](#)
- [the section called “\[Network Firewall.1\] Network firewalls sollten über mehrere Availability Zones hinweg bereitgestellt werden”](#)
- [the section called “\[Network Firewall.2\] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein”](#)
- [the section called “Auf \[Opensearch.10\] OpenSearch -Domains sollte das neueste Softwareupdate installiert sein”](#)
- [the section called “\[PCA.1\] AWS Private CA Root-Zertifizierungsstelle sollte deaktiviert sein”](#)
- [the section called “\[S3.19\] Bei S3-Zugriffspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein”](#)

- [the section called “\[S3.20\] Bei S3-Allzweck-Buckets sollte MFA Delete aktiviert sein”](#)

[Bereicherung finden](#)

Security Hub CSPM hat die neuen Finding-Felder `AwsAccountName` , `ApplicationArn` , und `ApplicationName` zum AWS Security Finding Format (ASFF) hinzugefügt.

8. November 2023

[Verbesserungen am Übersichts-Dashboard](#)

Sie können jetzt auf der Übersichtsseite der Security Hub CSPM-Konsole auf weitere Dashboard-Widgets zugreifen, Dashboard-Filterätze speichern, um sich schnell auf bestimmte Sicherheitsprobleme zu konzentrieren, und das Dashboard-Layout anpassen.

8. November 2023

[Zentrale Konfiguration](#)

Die zentrale Konfiguration ist jetzt verfügbar. Bei der zentralen Konfiguration kann der delegierte Security Hub CSPM-Administrator Security Hub CSPM, Standards und Kontrollen für mehrere Unternehmenskonten, Organisationseinheiten (OU) und Regionen konfigurieren.

8. November 2023

[Aktualisierungen der verwalteten Richtlinien](#)

Security Hub CSPM hat der `AWSSecurityHubServiceRolePolicy` verwalteten Richtlinie neue Berechtigungen hinzugefügt, die es Security Hub CSPM ermöglichen, anpassbare Eigenschaften der Sicherheitskontrolle zu lesen und zu aktualisieren.

26. November 2023

[Benutzerdefinierte Steuerungsparameter](#)

Sie können jetzt Parameterwerte für ausgewählte Security Hub CSPM-Steuerelemente anpassen. Dadurch können die Ergebnisse für eine bestimmte Kontrolle Ihren Geschäftsanforderungen und Sicherheitserwartungen besser entsprechen.

26. November 2023

[Aktualisierungen der verwalteten Richtlinien](#)

Security Hub CSPM hat die Richtlinien aktualisiert `AWSSecurityHubFullAccess` und `AWSSecurityHubOrganizationsAccess` verwaltet, mit denen Sie die Funktionen von Security Hub CSPM bzw. deren Integration nutzen können. AWS Organizations

16. November 2023

Bestehende Sicherheitskontrollen wurden zum Service-Managed Standard hinzugefügt: AWS Control Tower

Die folgenden vorhandenen Security Hub CSPM-Steuer-elemente wurden dem Service-Managed Standard hinzugefügt: AWS Control Tower

14. November 2023

- ACM.2
- AppSync.5.
- CloudTrail.6
- DMS.9
- DocumentDB DB.3
- DynamoDB.3
- EC2.2.3
- EKS.1
- ElastiCache.3.
- ElastiCache.4
- ElastiCache.5
- ElastiCache.6
- EventBridge.3.
- KMS.4
- Lambda.3
- MQ.5
- MQ.6
- MSK.1
- RDS.12
- RDS.15
- S 3,17

Aktualisierungen der verwalteten Richtlinien

Security Hub CSPM hat der `AWSecurityHubServiceRolePolicy` verwaltet en Richtlinie eine neue Tagging-Berechtigung hinzugefügt, die es Security Hub CSPM ermöglicht, Ressourcen-Tags zu lesen, die sich auf Ergebnisse beziehen.

7. November 2023

Neue Sicherheitskontrollen

Die folgenden neuen Security Hub CSPM-Steuerelemente sind verfügbar:

10. Oktober 2023

- the section called “[AppSync .5] AWS AppSync GraphQL APIs sollte nicht mit API-Schlüsseln authentifiziert werden”
- the section called “[DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein”
- the section called “[DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein”
- the section called “[DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein”
- the section called “[DMS.9] DMS-Endpunkte sollten SSL verwenden”
- the section called “[DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein”
- the section called “[DocumentDB.4] Amazon DocumentDB-Cluster sollten

Auditprotokolle in Logs veröffentlichen CloudWatch

”
–

- the section called
“[DocumentDB.5] Bei
Amazon DocumentD
B-Clustern sollte der
Löschschutz aktiviert sein”
- the section called “[ECS.9]
ECS-Aufgabendefini
tionen sollten über eine
Protokollierungskonfigurati
on verfügen”
- the section called “[EventBr
idge.3] An EventBrid
ge benutzerdefinierte
Eventbusse sollte eine
ressourcenbasierte Richtlini
e angehängt werden”
- the section called “[EventBr
idge.4] Auf EventBridge
globalen Endpunkten sollte
die Ereignisreplikation
aktiviert sein”
- the section called “[MSK.1]
MSK-Cluster sollten bei
der Übertragung zwischen
Broker-Knoten verschlüsselt
werden”
- the section called “[MQ.5]
ActiveMQ-Broker sollten den
Aktiv-/Standby-Bereitstellu
ngsmodus verwenden”
- the section called “[MQ.6]
RabbitMQ-Broker sollten

den Cluster-Bereitstellungsmodus verwenden”

- the section called “[Network Firewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein”
- the section called “[RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
”
–
- the section called “[RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein”
- the section called “[Route53 .2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren”
- the section called “Für [WAF.12] AWS WAF Regeln sollten Metriken aktiviert sein CloudWatch ”

[Aktualisierungen der verwalteten Richtlinien](#)

Security Hub CSPM hat der `AWSecurityHubServiceRolePolicy` verwaltet en Richtlinie neue Organisationsaktionen hinzugefügt, die es Security Hub CSPM ermöglichen, Konto- und Organisationseinheiteninformationen (OU) abzurufen. Wir haben auch neue Security Hub CSPM-Aktionen hinzugefügt, die es Security Hub CSPM ermöglichen, Dienstkonfigurationen, einschließlich Standards und Kontrollen, zu lesen und zu aktualisieren.

27. September 2023

Bestehende Sicherheitskontrollen wurden zum Service-Managed Standard hinzugefügt: AWS Control Tower

Die folgenden vorhandenen Security Hub CSPM-Steuer-elemente wurden dem Service-Managed Standard hinzugefügt: AWS Control Tower

26. September 2023

- the section called “[Athena.1] Athena-Arbeitsgruppen sollten im Ruhezustand verschlüsselt werden”
- the section called “[DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden”
- the section called “[DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen”
- the section called “[Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden”
- the section called “[Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
”
- the section called “[Neptune.3] Neptune-DB-Cluster -Snapshots sollten nicht öffentlich sein”

- [the section called “\[Neptune .4\] Bei Neptune-DB-Cluster n sollte der Löschschutz aktiviert sein”](#)
- [the section called “\[Neptune .5\] Bei Neptune-DB-Cluster n sollten automatische Backups aktiviert sein”](#)
- [the section called “\[Neptune .6\] Neptune-DB-Cluster -Snapshots sollten im Ruhezustand verschlüsselt werden”](#)
- [the section called “\[Neptune .7\] Bei Neptune-DB-Cluster n sollte die IAM-Daten bankauthentifizierung aktiviert sein”](#)
- [the section called “\[Neptune .8\] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren”](#)
- [the section called “\[RDS.27\] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden”](#)

[Ansicht konsolidierter Kontrollen und konsolidierte Kontrollergebnisse verfügbar in AWS GovCloud \(US\)](#)

Die Ansicht der konsolidierten Kontrollen und die konsolidierten Kontrollergebnisse sind jetzt in der verfügbar AWS GovCloud (US) Region. Auf der Seite „Kontrollen“ der Security Hub CSPM-Konsole werden all Ihre Kontrollen standardübergreifend angezeigt. Jede Kontrolle hat standardübergreifend dieselbe Kontroll-ID. Wenn Sie konsolidierte Kontrollergebnisse aktivieren, erhalten Sie ein einziges Ergebnis pro Sicherheitsprüfung, auch wenn eine Kontrolle für mehrere aktivierte Standards gilt.

6. September 2023

[Ansicht konsolidierter Kontrollen und konsolidierte Kontrollergebnisse in den Regionen China verfügbar](#)

Die Ansicht der konsolidierten Kontrollen und die konsolidierten Kontrollergebnisse sind jetzt in den Regionen China verfügbar. Auf der Seite „Kontrollen“ der Security Hub CSPM-Konsole werden all Ihre Kontrollen standardübergreifend angezeigt. Jede Kontrolle hat standardübergreifend dieselbe Kontroll-ID. Wenn Sie konsolidierte Kontrollergebnisse aktivieren, erhalten Sie ein einziges Ergebnis pro Sicherheitsprüfung, auch wenn eine Kontrolle für mehrere aktivierte Standards gilt.

28. August 2023

[Security Hub CSPM in der Region Israel \(Tel Aviv\) verfügbar](#)

Security Hub CSPM ist jetzt in Israel (Tel Aviv) verfügbar. Alle Security Hub CSPM-Funktionen sind jetzt in dieser Region verfügbar, mit Ausnahme bestimmter Sicherheitskontrollen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

08. August 2023

Neue Sicherheitskontrollen

Die folgenden neuen Security Hub CSPM-Steuererelemente sind verfügbar:

28. Juli 2023

- the section called “[Athena.1] Athena-Arbeitsgruppen sollten im Ruhezustand verschlüsselt werden”
- the section called “[DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden”
- the section called “[DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen”
- the section called “[Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden”
- the section called “[Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch”
–
- the section called “[Neptune.3] Neptune-DB-Cluster -Snapshots sollten nicht öffentlich sein”
- the section called “[Neptune.4] Bei Neptune-DB-Cluster

n sollte der Löschschutz
aktiviert sein”

- the section called “[Neptune
.5] Bei Neptune-DB-Cluster
n sollten automatische
Backups aktiviert sein”
- the section called “[Neptune
.6] Neptune-DB-Cluster
-Snapshots sollten im
Ruhezustand verschlüsselt
werden”
- the section called “[Neptune
.7] Bei Neptune-DB-Cluster
n sollte die IAM-Daten
bankauthentifizierung
aktiviert sein”
- the section called “[Neptune
.8] Neptune-DB-Cluster
sollten so konfiguriert sein,
dass sie Tags in Snapshots
kopieren”
- the section called “[RDS.27]
RDS-DB-Cluster sollten im
Ruhezustand verschlüsselt
werden”

Neue Operatoren für Kriterien für Automatisierungsregeln

Sie können jetzt die Vergleichsoperatoren CONTAINS und NOT_CONTAINS für die Zuordnung von Automatisierungsregeln und Zeichenkettenkriterien verwenden.

25. Juli 2023

[Automatisierungsregeln](#)

Security Hub CSPM bietet jetzt 13. Juni 2023
Automatisierungsregeln, die
Ergebnisse auf der Grundlage
der von Ihnen angegebenen
Kriterien automatisch aktualisi-
eren.

[Neue Integration von Drittanbi-
etern](#)

Snyk ist eine neue Drittanbi- 12. Juni 2023
eter-Integration, die Ergebniss-
e an Security Hub CSPM
sendet.

Bestehende Sicherheitskontrollen wurden dem Service-Managed Standard hinzugefügt: AWS Control Tower

Die folgenden vorhandenen Security Hub CSPM-Steuer-elemente wurden dem Service-Managed Standard hinzugefügt: AWS Control Tower

12. Juni 2023

- the section called “[Account .1] Sicherheitskontakt informationen sollten bereitgestellt werden für AWS-Konto”
- the section called “[APIGateway.8] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben”
- the section called “[APIGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein”
- the section called “[CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein”
- the section called “[EC2.25] EC2 Amazon-Startvorlagen sollten Netzwerkschnittstellen nicht öffentlich IPs zuweisen”
- the section called “[ELB.1] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden”

- the section called “[Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden”
- the section called “[SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden”
- the section called “[SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben”
- the section called “[WAF.10] AWS WAF web ACLs sollte mindestens eine Regel oder Regelgruppe haben”

Neue Sicherheitskontrollen

Die folgenden neuen Security Hub CSPM-Steuerelemente sind verfügbar:

6. Juni 2023

- the section called “[ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden”
- the section called “[AppSync .2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben”
- the section called “[CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden”
- the section called “[Elastic Beanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch”
- the section called “[S3.17] S3-Allzweck-Buckets sollten im Ruhezustand verschlüsselt werden mit AWS KMS keys”
- the section called “[StepFunctions.1] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben”

[Security Hub CSPM im
asiatisch-pazifischen Raum
\(Melbourne\) verfügbar](#)

Security Hub CSPM ist jetzt im asiatisch-pazifischen Raum (Melbourne) verfügbar. Alle Security Hub CSPM-Funktionen sind jetzt in dieser Region verfügbar, mit Ausnahme bestimmter Sicherheitskontrollen. Weitere Informationen finden Sie unter [Verfügbarkeit von Kontrollen nach Regionen](#).

25. Mai 2023

[Verlauf finden](#)

Security Hub CSPM kann jetzt den Verlauf eines Fundes in den letzten 90 Tagen verfolgen.

4. Mai 2023

Neue Sicherheitskontrollen

Die folgenden neuen Security Hub CSPM-Steuerelemente sind verfügbar:

29. März 2023

- [the section called “\[EKS.1\] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein”](#)
- [the section called “\[ELB.16\] Application Load Balancers sollten mit einer Web-ACL verknüpft sein AWS WAF”](#)
- [the section called “\[Redshift.10\] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden”](#)
- [the section called “\[S3.15\] Bei S3-Allzweck-Buckets sollte Object Lock aktiviert sein”](#)

Erweiterte Unterstützung für konsolidierte Kontrollergebnisse

Die [automatisierte Sicherheitsreaktion auf AWS Version 2.0.0](#) unterstützt jetzt konsolidierte Kontrollergebnisse.

24. März 2023

Security Hub CSPM in neuer Version erhältlich AWS-Regionen

Security Hub CSPM ist jetzt im asiatisch-pazifischen Raum (Hyderabad), Europa (Spanien) und Europa (Zürich) verfügbar. In diesen Regionen gibt es Beschränkungen, welche Kontrollen verfügbar sind.

21. März 2023

[Aktualisierung der verwalteten Richtlinie](#)

Security Hub CSPM hat eine bestehende Berechtigung in der `AWSecurityHubServiceRolePolicy` verwalteten Richtlinie aktualisiert.

17. März 2023

Neue Sicherheitskontrollen für den NIST 800-53-Standard

Security Hub CSPM hat die folgenden Sicherheitskontrollen hinzugefügt, die für den NIST 800-53-Standard gelten:

03. März 2023

- the section called “[Account .2] AWS-Konten sollte Teil einer Organisation sein AWS Organizations”
- the section called “[CloudWatch.15] Für CloudWatch Alarme sollten bestimmte Aktionen konfiguriert sein”
- the section called “[CloudWatch.16] CloudWatch Protokollgruppen sollten für einen bestimmten Zeitraum aufbewahrt werden”
- the section called “[CloudWatch.17] CloudWatch Alarmaktionen sollten aktiviert sein”
- the section called “[DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein”
- the section called “[EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt sein”
- EC2.29 — EC2 Instances sollten in einer VPC gestartet werden (eingestellt)

- [the section called “\[RDS.26\] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden”](#)
- [the section called “\[S3.14\] Für S3-Allzweck-Bucket s sollte die Versionierung aktiviert sein”](#)
- [the section called “\[WAF.11\] Die AWS WAF Web-ACL-P rotokollierung sollte aktiviert sein”](#)

[Nationales Institut für Standards und Technologie \(NIST\) 800-53 Rev. 5](#)

Security Hub CSPM unterstützt jetzt den Standard NIST 800-53 Rev. 5 mit mehr als 200 anwendbaren Sicherheitskontrollen.

28. Februar 2023

[Konsolidierte Kontrollen: Ergebnisse anzeigen und kontrollieren](#)

Mit der Veröffentlichung der konsolidierten Kontrollansicht werden auf der Seite „Kontrollen“ der Security Hub CSPM-Konsole all Ihre Kontrollen standardübergreifend angezeigt. Jede Kontrolle hat standardübergreifend dieselbe Kontroll-ID. Wenn Sie konsolidierte Kontrolle ergebnisse aktivieren, erhalten Sie ein einziges Ergebnis pro Sicherheitsprüfung, auch wenn eine Kontrolle für mehrere aktivierte Standards gilt.

23. Februar 2023

Neue Sicherheitskontrollen

Die folgenden neuen Security Hub CSPM-Steuer-elemente sind verfügbar. Für einige Kontrollen gelten [regionale](#) Einschränkungen.

16. Februar 2023

- [the section called “Bei \[ElastiCache.1\] ElastiCache \(Redis OSS\) -Clustern sollten automatische Backups aktiviert sein”](#)
- [the section called “\[ElastiCache.2\] Bei ElastiCache Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein”](#)
- [the section called “\[ElastiCache.3\] Für ElastiCache Replikationsgruppen sollte der automatische Failover aktiviert sein”](#)
- [the section called “\[ElastiCache.4\] ElastiCache Replikationsgruppen sollten im Ruhezustand verschlüsselt werden”](#)
- [the section called “\[ElastiCache.5\] ElastiCache Replikationsgruppen sollten bei der Übertragung verschlüsselt werden”](#)
- [the section called “\[ElastiCache.6\] Für Replikationsgruppen ElastiCache \(Redis OSS\) früherer](#)

[Versionen sollte Redis OSS AUTH aktiviert sein](#)

- [the section called "\[Elasticache.7\] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden"](#)

[Neue ASFF-Felder](#)

Security Hub CSPM wurde hinzugefügt. ProductFields ArchivalReasonsSecurity Hub ProductFields CSPM wurde hinzugefügt. ---- SEP----:0/Description und. ArchivalReasons:0/Description ReasonCode und. AWS ---- sep----:0/ zum Security Finding Format (ASFF).

8. Februar 2023

[Neue ASFF-Felder](#)

Security Hub CSPM hat Compliance hinzugefügt. AssociatedStandards und Compliance. SecurityControlld zum AWS Security Finding Format (ASFF).

31. Januar 2023

[Details zur Sicherheitslücke sind jetzt verfügbar](#)

Sie können jetzt in der Security Hub CSPM-Konsole Details zu Sicherheitslücken für Ergebnisse sehen, die Amazon Inspector an Security Hub CSPM sendet.

14. Januar 2023

[Security Hub CSPM ist im Mittleren Osten \(VAE\) verfügbar](#)

Security Hub CSPM ist jetzt im Mittleren Osten (VAE) verfügbar. Für einige Kontrollen gelten regionale Beschränkungen.

12. Januar 2023

[Integration von Drittanbietern mit hinzugefügt MetricStream](#)

Security Hub CSPM unterstützt jetzt die Integration von Drittanbietern MetricStream in allen Regionen außer China und. AWS GovCloud (US)

11. Januar 2023

[Das Limit für Unternehmenskonten wurde erhöht](#)

Security Hub CSPM unterstützt jetzt bis zu 11.000 Mitgliedskonten für jedes Security Hub CSPM-Administratorkonto pro Region.

27. Dezember 2022

[ElasticBeanstalk1.3 wurde zurückgesetzt](#)

Security Hub CSPM hat die Kontrolle rückgängig gemacht [ElasticBeanstalk. 3] Elastic Beanstalk sollte in allen Regionen Logs CloudWatch vom FSBP-Standard streamen.

21. Dezember 2022

[Security Hub CSPM fügt neue Sicherheitskontrollen hinzu](#)

Neue Security Hub CSPM-Steuerelemente stehen Kunden zur Verfügung, die den FSBP-Standard aktiviert haben. [Für einige Kontrollen gelten regionale Einschränkungen.](#)

15. Dezember 2022

[Hinweise zu kommenden Funktionen](#)

Security Hub CSPM plant die Veröffentlichung von zwei neuen Funktionen: konsolidierte Kontrollansicht und konsolidierte Kontrolle rgebnisse. Diese kommenden Funktionen können sich auf bestehende Workflows auswirken, die auf Feldern und Werten zur Kontrollermittlung basieren.

9. Dezember 2022

[Amazon Security Lake-Integration jetzt verfügbar](#)

Security Lake lässt sich jetzt in Security Hub CSPM integrieren, indem es die Ergebniss e von Security Hub CSPM empfängt.

29. November 2022

[Support für Service-Managed Standard: AWS Control Tower](#)

Security Hub CSPM unterstüt zt einen neuen Sicherhei tsstandard namens Service-Managed Standard:. AWS Control Tower AWS Control Tower verwaltet diesen Standard.

28. November 2022

[CIS AWS Foundations Benchmark v1.4.0 jetzt in China Regionen verfügbar](#)

Security Hub CSPM unterstüt zt jetzt den CIS AWS Foundations Benchmark v1.4.0 in den Regionen China.

18. November 2022

[Die Cloud-Integration von Jira Service Management ist jetzt verfügbar](#)

Jira Service Management Cloud erhält jetzt CSPM-Ergebnisse von Security Hub in allen verfügbaren Regionen außer den Regionen China.

17. November 2022

[AWS IoT Device Defender
Integration jetzt verfügbar](#)

AWS IoT Device Defender sendet jetzt Ergebnisse an Security Hub CSPM in allen verfügbaren Regionen.

17. November 2022

[Support für CIS AWS
Foundations Benchmark
v1.4.0](#)

Security Hub CSPM bietet jetzt Sicherheitskontrollen, die den CIS AWS Foundations Benchmark v1.4.0 unterstützen. Dieser Standard ist in allen verfügbaren Regionen mit Ausnahme der Regionen China verfügbar.

9. November 2022

[Support für Security Hub
CSPM-Ankündigungen in
AWS GovCloud \(US\)](#)

Sie können jetzt Security Hub CSPM-Ankündigungen mit Amazon Simple Notification Service (Amazon SNS) in (USA-Ost) und AWS GovCloud AWS GovCloud (US-West) abonnieren, um Benachrichtigungen über Security Hub CSPM zu erhalten.

3. Oktober 2022

[AWS Security Hub Cloud
Security Posture Management \(CSPM\) fügt eine neue
Sicherheitskontrolle hinzu](#)

Das neue Security Hub CSPM Control AutoScaling.9 steht Kunden zur Verfügung, die den FSBP-Standard aktiviert haben. [Die Kontrollen können regionalen Einschränkungen unterliegen.](#)

01. September 2022

[Abonnieren Sie die CSPM-Ankündigungen von Security Hub](#)

Sie können jetzt Security Hub CSPM-Ankündigungen mit Amazon Simple Notification Service (Amazon SNS) abonnieren, um Benachrichtigungen über Security Hub CSPM zu erhalten.

2p. August 2022

[Regionserweiterung für regionsübergreifende Aggregation](#)

Die regionsübergreifende Aggregation ist jetzt für Ergebnisse, Aktualisierungen und Einblicke in alle Regionen verfügbar. AWS GovCloud (US)

02. August 2022

[Neue Produktintegrationen von Drittanbietern](#)

Fortinet — FortiCNP ist eine Drittanbieter-Integration, die Security Hub CSPM-Ergebnisse empfängt, und JFrog ist eine Drittanbieter-Integration, die Ergebnisse an Security Hub CSPM sendet.

26. Juli 2022

[EC2.7 ist im Ruhestand](#)

Security Hub CSPM wurde eingestellt EC2.27 — Laufende EC2 Instances sollten keine Schlüsselpaare verwenden, eine frühere Kontrolle im Standard AWS Foundational Security Best Practices (FSBP).

20. Juli 2022

Lambda.2 unterstützt Python3.6 nicht mehr	Security Hub CSPM unterstützt Python3.6 nicht mehr als Parameter für Lambda.2 — Lambda-Funktionen sollten unterstützte Laufzeiten verwenden, eine Steuerung im Standard Foundational Security Best Practices (FSBP). AWS	19. Juli 2022
AWS Security Hub Cloud Security Posture Management (CSPM) fügt neue Sicherheitskontrollen hinzu	Neue Security Hub CSPM-Steuerelemente stehen Kunden zur Verfügung, die den FSBP-Standard aktiviert haben. Für einige Kontrollen gelten regionale Einschränkungen.	22. Juni 2022
AWS Security Hub Cloud Security Posture Management (CSPM) unterstützt eine neue Region	Security Hub CSPM ist jetzt im asiatisch-pazifischen Raum (Jakarta) verfügbar. Einige Steuerelemente sind in dieser Region nicht verfügbar.	7. Juni 2022
Verbesserte Integration zwischen AWS Security Hub Cloud Security Posture Management (CSPM) und AWS Config	Security Hub CSPM-Benutzer können die Ergebnisse der AWS Config Regelauswertungen als Ergebnisse in Security Hub CSPM sehen.	6. Juni 2022

<u>Es wurde die Möglichkeit hinzugefügt, automatisch aktivierte Standards zu deaktivieren</u>	Für Benutzer, die mit integriert sind AWS Organizations, ermöglicht diese Funktion, sich beim Security Hub CSPM-Administratorkonto anzumelden und neue Mitgliedskonten von den automatisch aktivierten Standards abzumelden.	25. April 2022
<u>Erweiterte regionsübergreifende Aggregation</u>	Es wurde eine regionsübergreifende Aggregation hinzugefügt, um Status und Sicherheitsbewertungen zu kontrollieren.	20. April 2022
<u>CompanyName und ProductName sind jetzt Attribute der obersten Ebene</u>	Es wurden neue Attribute der obersten Ebene hinzugefügt, um Firmen- und Produktnamen für benutzerdefinierte Integrationen festzulegen	1. April 2022
<u>Dem Standard „Best Practices für AWS grundlegende Sicherheit“ wurden neue Kontrollen hinzugefügt</u>	Der Standard „Best Practices“ von AWS Foundational Security wurde um 5 neue Kontrollen erweitert.	31. März 2022
<u>ASFF wurde um neue Objekte mit Ressourcendetails erweitert</u>	AwsRdsDbSecurityGroup Ressourcentyp zu ASFF hinzugefügt.	25. März 2022
<u>Zusätzliche Ressourcendetails in ASFF hinzugefügt</u>	Zusätzliche Details zu <code>AwsAutoScalingScalingGroup</code> , <code>AwsElbLoadBalancer</code> , <code>AwsRedshiftCluster</code> , und <code>AwsCodeBuildProject</code> hinzugefügt.	25. März 2022

[Dem Standard „Bewährte Methoden für AWS grundlegende Sicherheit“ wurden neue Steuerelemente hinzugefügt](#)

Der Standard „Best Practices“ von AWS Foundational Security wurde um 15 neue Kontrollen erweitert.

16. März 2022

[Dem AWS Foundational Security Best Practices-Standard und dem Payment Card Industry Data Security Standard \(PCI DSS\) wurden neue Kontrollen hinzugefügt](#)

Neue Steuerelemente für Amazon OpenSearch Service, Amazon RDS, Amazon EC2, Elastic Load Balancing und CloudFront zum Standard „Best Practices für AWS grundlegende Sicherheit“ hinzugefügt. Außerdem wurden dem PCI DSS zwei neue Steuerungen für OpenSearch Service hinzugefügt.

15. Februar 2022

[ASFF wurde ein neues Feld hinzugefügt](#)

Neues Feld hinzugefügt: Beispiel.

26. Januar 2022

[Integration mit hinzugefügt AWS Health](#)

AWS Health verwendet service-to-service Ereignisnachrichten, um Ergebnisse an Security Hub CSPM zu senden.

19. Januar 2022

[Integration mit hinzugefügt AWS Trusted Advisor](#)

Trusted Advisor sendet die Ergebnisse seiner Prüfungen als Security Hub CSPM-Ergebnisse an Security Hub CSPM. Security Hub CSPM sendet die Ergebnisse seiner AWS Foundational Security Best Practices-Prüfungen an Trusted Advisor

18. Januar 2022

Objekte mit Ressourcendetails in ASFF wurden aktualisiert

MixedInstancesPolicy und AvailabilityZones wurden zu AwsAutoScalingAutoScalingGroup hinzugefügt. Hinzufügung von MetadataOptions zu AwsAutoScalingLaunchConfiguration . Hinzufügung von BucketVersioningConfiguration zu AwsS3Bucket .

20. Dezember 2021

Die Ausgabe für die ASFF-Dokumentation wurde aktualisiert

Die Beschreibungen der ASFF-Attribute waren zuvor in einem einzigen Thema zusammengefasst. Jedes Objekt der obersten Ebene und jedes Objekt mit Ressourcendetails befindet sich jetzt in einem eigenen Thema. Das Thema ASFF-Syntax enthält Links zu diesen Themen.

20. Dezember 2021

ASFF wurde um neue Objekte mit Ressourcendetails erweitert für AWS Network Firewall

For AWS Network Firewall hat die folgenden Objekte mit Ressourcendetails hinzugefügt: AwsNetworkFirewallFirewall AwsNetworkFirewallPolicy , und AwsNetworkFirewallRuleGroup .

20. Dezember 2021

[Unterstützung für die neue Version von Amazon Inspector hinzugefügt](#)

Security Hub CSPM ist in die neue Version von Amazon Inspector sowie in Amazon Inspector Classic integriert. Amazon Inspector sendet Ergebnisse an Security Hub CSPM.

29. November 2021

[Der Schweregrad von 1,9 wurde geändert EC2](#)

Der Schweregrad von EC2 .19 (Sicherheitsgruppen sollten keinen uneingeschränkten Zugriff auf Ports mit hohem Risiko zulassen) wurde von Hoch auf Kritisch geändert.

17. November 2021

[Neue Integration mit Sonrai Dig](#)

Security Hub CSPM bietet jetzt eine Integration mit Sonrai Dig. Sonrai Dig überwacht Cloud-Umgebungen, um Sicherheitsrisiken zu identifizieren. Sonrai Dig sendet Ergebnisse an Security Hub CSPM.

12. November 2021

[Die Prüfung auf CIS 2.1- und CloudTrail 7.1-Steurelemente wurde aktualisiert](#)

CIS 2.1 und CloudTrail .1 überprüfen jetzt nicht nur, ob mindestens ein CloudTrail Multi-Region-Tail vorhanden ist, sondern überprüfen nun auch, ob der ExcludeManagementEventSources Parameter in mindestens einem der CloudTrail Multi-Region-Wanderwege leer ist.

9. November 2021

Unterstützung für VPC-Endpunkte hinzugefügt	Security Hub CSPM ist jetzt in VPC-Endpunkte integriert AWS PrivateLink und unterstützt diese.	3. November 2021
Dem Standard „Best Practices für AWS grundlegende Sicherheit“ wurden zusätzliche Kontrollen hinzugefügt	Neue Steuerelemente für Elastic Load Balancing (ELB.2 und ELB.8) und AWS Systems Manager (SSM.4) hinzugefügt.	2. November 2021
Es wurden Ports zur Prüfung für das 1.9-Steuerelement hinzugefügt EC2	EC2.19 überprüft jetzt auch, ob Sicherheitsgruppen keinen uneingeschränkten Eingangszugriff auf die folgenden Ports zulassen: 3000 (Go, Node.js und Ruby Web Development Frameworks), 5000 (Python Web Development Frameworks), 8088 (Legacy-HTTP-Port) und 8888 (alternativer HTTP-Port)	27. Oktober 2021
Die Integration mit Logz.io Cloud SIEM wurde hinzugefügt	Logz.io ist ein Anbieter von Cloud-SIEM, der eine erweiterte Korrelation von Protokoll- und Ereignisdaten ermöglicht, um Sicherheitsteams dabei zu unterstützen, Sicherheitsbedrohungen in Echtzeit zu erkennen, zu analysieren und darauf zu reagieren. Logz.io erhält Ergebnisse von Security Hub CSPM.	25. Oktober 2021

[Unterstützung für die
regionsübergreifende
Aggregation von Ergebnissen
hinzugefügt](#)

Durch die regionsübergreifen
de Aggregation können Sie
sich alle Ihre Ergebnisse
ansehen, ohne die Regionen
ändern zu müssen. Administr
atorkonten wählen eine
Aggregationsregion und
verknüpfte Regionen aus.
Die Ergebnisse für das
Administratorkonto und seine
Mitgliedskonten werden von
den verknüpften Regionen
zur Aggregationsregion
zusammengefasst.

20. Oktober 2021

[Objekte mit Ressourcendetails
in ASFF wurden aktualisiert](#)

Details zum Viewer-Ze
rtifikat wurden hinzugefügt.
AwsCloudFrontDistr
ibution Zusätzliche
Details wurden hinzugefü
gtAwsCodeBuildProjec
t . Load Balancer-Attribute
wurden hinzugefügt
zuAwsElbV2LoadBalanc
er . Die Konto-ID des S3-
Bucket-Besitzers wurde
hinzugefügt. AwsS3Bucket

8. Oktober 2021

[Neue Objekte mit Ressourcendetails zu ASFF hinzugefügt](#)

Die folgenden neuen Ressourcendetailobjekte wurden zu ASFF hinzugefügt: `AwsEc2VpcEndpointService`, `AwsEcrRepository`, `AwsEksCluster`, `AwsOpenSearchServiceDomain`, `AwsWafRateBasedRule`, `AwsWafRegionalRateBasedRule`, `AwsXrayEncryptionConfig`

8. Oktober 2021

[Veraltete Runtime aus dem Lambda.2-Steuerement entfernt](#)

Im Standard „Best Practices für AWS grundlegende Sicherheit“ wurde die `dotnetcore2.1` Laufzeit aus [Lambda.2] entfernt. Lambda-Funktionen sollten unterstützte Laufzeiten verwenden.

6. Oktober 2021

[Neuer Name für die Check Point-Integration](#)

Die Integration mit Check Point Dome9 Arc heißt jetzt Check Point CloudGuard Posture Management. Der Integrations-ARN hat sich nicht geändert.

1. Oktober 2021

[Die Integration mit Alcide wurde entfernt](#)

Die Integration mit Alcide KAudit wurde eingestellt.

30. September 2021

[Der Schweregrad von 1,9 wurde geändert EC2](#)

Der Schweregrad von [EC2.19] Sicherheitsgruppen sollten keinen uneingeschränkten Zugriff auf Ports mit hohem Risiko zulassen, wurde von Mittel auf Hoch geändert.

30. September 2021

[Die Integration mit AWS Organizations wird jetzt in den Regionen China unterstützt](#)

Die Security Hub CSPM-Integration mit Organizations wird jetzt in China (Peking) und China (Ningxia) unterstützt.

20. September 2021

[Neue AWS Config Regel für die Steuerungen S3.1 und PCI.S3.6](#)

Sowohl S3.1 als auch PCI.S3.6 stellen sicher, dass die Amazon S3 S3-Einstellung Block Public Access aktiviert ist. Die AWS Config Regel für diese Steuerelemente wurde von auf geändert. s3-account-level-public-access-blocks s3-account-level-public-access-blocks-periodic

14. September 2021

[Veraltete Laufzeiten wurden aus dem Lambda.2-Steuerelement entfernt](#)

Im Standard „Best Practices für AWS grundlegende Sicherheit“ wurden die ruby2.5 Laufzeiten nodejs10.x und aus [Lambda.2] entfernt. Lambda-Funktionen sollten unterstützte Laufzeiten verwenden.

13. September 2021

[Der Schweregrad der CIS 2.2-Steuerung wurde geändert](#)

Im Benchmark-Standard der CIS AWS Foundations ist dies der Schweregrad für 2.2. — Stellen CloudTrail Sie sicher, dass die Validierung der Protokolldatei von Niedrig auf Mittel aktiviert ist.

13. September 2021

[ECS.1, Lambda.2 und SSM.1 im Standard „Best Practices für grundlegende Sicherheit“ aktualisiert AWS](#)

Im Standard AWS Foundational Security Best Practices hat ECS.1 jetzt einen Parameter, der auf `skipInactiveTaskDefinitions` `true` ist. Dadurch wird sichergestellt, dass das Steuerelement nur aktive Aufgabendefinitionen überprüft. Für Lambda.2 wurde Python 3.9 zur Liste der Laufzeiten hinzugefügt. SSM.1 überprüft jetzt sowohl gestoppte als auch laufende Instanzen.

7. September 2021

[Die PCI.Lambda.2-Steuerung schließt jetzt Lambda @Edge -Ressourcen aus](#)

Im Payment Card Industry Data Security Standard (PCI DSS) -Standard schließt die PCI.Lambda.2-Steuerung nun Lambda @Edge -Ressourcen aus.

7. September 2021

[Die Integration mit wurde hinzugefügt HackerOne Vulnerability Intelligence](#)

Security Hub CSPM bietet jetzt eine Integration mit HackerOne Vulnerability Intelligence. Die Integration sendet die Ergebnisse an Security Hub CSPM.

7. September 2021

[Objekte mit Ressourcendetails in ASFF wurden aktualisiert](#)

Für `AwsKmsKey` , hinzugefügt `KeyRotationStatus` .
Für `AwsS3Bucket` , hinzugefügt `AccessControlList` `BucketLoggingConfiguration` , `BucketNotificationConfiguration` , und `BucketWebsiteConfiguration` .

2. September 2021

[ASFF wurde um neue Objekte mit Ressourcendetails erweitert](#)

ASFF wurde um die folgenden neuen Objekte mit Ressourcendetails erweitert: `AwsAutoScalingLaunchConfiguration` `AwsEc2VpnConnection` , und `AwsEcrContainerImage`

2. September 2021

[Dem `Vulnerabilities` Objekt in ASFF wurden Details hinzugefügt](#)

In `Cvss`, hinzugefügt `Adjustments` und `Source`.
`VulnerablePackages` In wurden der Dateipfad und der Paketmanager hinzugefügt.

2. September 2021

[Systems Manager Explorer und OpsCenter Integration werden jetzt in den Regionen China unterstützt](#)

Der Security Hub ist CSPM-Integration mit SSM Explorer und OpsCenter wird jetzt in China (Peking) und China (Ningxia) unterstützt.

31. August 2021

[Lambda.4-Steuerung außer Betrieb nehmen](#)

Security Hub CSPM stellt die Steuerung ein [Lambda.4] Für Lambda-Funktionen sollte eine Warteschlange für unzustellbare Briefe konfiguriert sein. Wenn ein Steuerelement außer Betrieb genommen wird, wird es nicht mehr auf der Konsole angezeigt, und Security Hub CSPM führt keine Prüfungen daran durch.

31. August 2021

[Die PCI wird außer Betrieb genommen. EC2.3. Steuerung](#)

Security Hub CSPM stellt die Steuerung ein [PCI. EC2.3] Ungenutzte EC2 Sicherheitsgruppen sollten entfernt werden. Wenn ein Steuerelement außer Betrieb genommen wird, wird es nicht mehr auf der Konsole angezeigt, und Security Hub CSPM führt keine Prüfungen daran durch.

27. August 2021

[Änderung der Art und Weise, wie Security Hub CSPM Ergebnisse an benutzerdefinierte Aktionen sendet](#)

Wenn Sie Ergebnisse an eine benutzerdefinierte Aktion senden, sendet Security Hub CSPM jetzt jedes Ergebnis in einem separaten Security Hub Findings - Custom ActionEreignis.

20. August 2021

[Es wurde ein neuer Code zur Begründung des Compliance-Status für benutzerdefinierte Lambda-Laufzeiten hinzugefügt](#)

Ein neuer Code für die Gründe für den LAMBDA_COMPLIANCE_STATUS_NOT_AVAILABLE Compliance-Status wurde hinzugefügt. Dieser Ursachecode weist darauf hin, dass Security Hub CSPM keine Prüfung anhand einer benutzerdefinierten Lambda-Laufzeit durchführen konnte.

20. August 2021

[AWS Firewall Manager Integration wird jetzt in den Regionen China unterstützt](#)

Die Security Hub CSPM-Integration mit Firewall Manager wird jetzt in China (Peking) und China (Ningxia) unterstützt.

19. August 2021

[Neue Integrationen mit und Caveonix CloudForcepoint Cloud Security Gateway](#)

Security Hub CSPM bietet jetzt Integrationen mit und Caveonix Cloud Forcepoint Cloud Security Gateway. Beide Integrationen senden die Ergebnisse an Security Hub CSPM.

10. August 2021

[Neue AttributeCompanyName, und Region wurden zu ProductName ASFF hinzugefügt](#)

RegionFelder CompanyName ProductName, und wurden zur obersten Ebene der ASFF hinzugefügt. Diese Felder werden automatisch ausgefüllt und können, mit Ausnahme von benutzerdefinierten Produktintegrationen, nicht mit BatchImportFindings oder aktualisiert werden. BatchUpdateFindings Auf der Konsole werden beim Suchen nach Filtern diese neuen Felder verwendet. In der API verwenden die ProductName Filter CompanyName und die Attribute, die sich unter befindenProductFields.

23. Juli 2021

[Objekte mit Ressourcendetails in ASFF hinzugefügt und aktualisiert](#)

Ein neuer AwsRdsEventSubscription Ressourcentyp und Ressourcendetails wurden hinzugefügt. Ressourcendetails für den AwsEcsService Ressourcentyp hinzugefügt. Dem Objekt mit den AwsElasticsearchDomain Ressourcendetails wurden Attribute hinzugefügt.

23. Juli 2021

[Dem Standard „Best Practices für AWS grundlegende Sicherheit“ wurden Kontrollen hinzugefügt](#)

Neue Steuerelemente für Amazon API Gateway (APIGateway.5), Amazon (EC2.19), Amazon ECS EC2 (ECS.2), Elastic Load Balancing (ELB.7), Amazon OpenSearch Service (ES.5 bis ES.8), Amazon RDS (RDS.16 bis RDS.23), Amazon Redshift (Redshift.4) und Amazon SQS (SQS.1) hinzugefügt.

20. Juli 2021

[Eine Berechtigung wurde innerhalb der mit dem Dienst verknüpften, rollenverwalteten Richtlinie verschoben](#)

Die `config:PutEvaluation` Berechtigung wurde innerhalb der verwalteten Richtlinie verschoben `nAWSSecurityHubServiceRolePolicy`, sodass sie auf alle Ressourcen angewendet wird.

14. Juli 2021

[Dem Standard „Bewährte Methoden für AWS grundlegende Sicherheit“ wurden Kontrollen hinzugefügt](#)

Neue Steuerelemente für Amazon API Gateway (APIGateway.4), Amazon (CloudFront.5 und CloudFront.6), Amazon CloudFront (EC2.17 und EC2.18), Amazon ECS EC2 (ECS.1), Amazon OpenSearch Service (ES.4), (IAM.21), Amazon RDS (RDS.15) und Amazon S3 AWS Identity and Access Management (S3.8) hinzugefügt.

8. Juli 2021

[Es wurden neue Begründungscodes für den Compliance-Status für Kontrollergebnisse hinzugefügt](#)

INTERNAL_SERVICE_ERROR weist darauf hin, dass ein unbekannter Fehler aufgetreten ist. SNS_TOPIC_CROSS_ACCOUNT gibt an, dass das SNS-Thema einem anderen Konto gehört. SNS_TOPIC_INVALID gibt an, dass das zugehörige SNS-Thema ungültig ist.

6. Juli 2021

[Die Integration mit Amazon Q Developer in Chat-Anwendungen wurde hinzugefügt](#)

Die Integration mit Amazon Q Developer in Chat-Anwendungen wurde hinzugefügt. Security Hub CSPM sendet Ergebnisse in Chat-Anwendungen an Amazon Q Developer.

30. Juni 2021

[Der mit dem Dienst verknüpften Richtlinie zur Verwaltung von Rollen wurde eine neue Berechtigung hinzugefügt](#)

Der verwalteten Richtlinie wurde eine neue Berechtigung hinzugefügt `AWSecurityHubServiceRolePolicy`, damit die dienstbezogene Rolle Bewertungsergebnisse liefern kann. AWS Config

29. Juni 2021

[Neue und aktualisierte Objekte mit Ressourcendetails im ASFF](#)

Neue Ressourcendetailobjekte für ECS-Cluster und ECS-Aufgabendefinitionen hinzugefügt. Das EC2 Instanzobjekt wurde aktualisiert und listet nun die zugehörigen Netzwerkschnittstellen auf. Die Client-Zertifikat-ID für die API Gateway V2-Stufen wurde hinzugefügt. Die Lebenszykluskonfiguration für S3-Buckets wurde hinzugefügt.

24. Juni 2021

[Die Berechnung der aggregierten Kontrollstatus und der Standardsicherheitsbewertungen wurde aktualisiert](#)

Security Hub CSPM berechnet jetzt alle 24 Stunden den Gesamtkontrollstatus und die Standardsicherheitsbewertung. Bei Administratorkonten spiegelt die Bewertung nun wider, ob die einzelnen Kontrollen für jedes Konto aktiviert oder deaktiviert sind.

23. Juni 2021

[Aktualisierte Informationen zum Umgang mit gesperrten Konten durch Security Hub CSPM](#)

Es wurden Informationen darüber hinzugefügt, wie Security Hub CSPM mit Konten umgeht, die gesperrt wurden. AWS

23. Juni 2021

[Es wurden Tabs hinzugefügt, um die aktivierten und deaktivierten Steuerelemente für das einzelne Administratorkonto anzuzeigen](#)

Für das Administratorkonto enthalten die Hauptregister auf der Standarddetailseite aggregierte Informationen für alle Konten. Auf den neuen Registerkarten Aktiviert für dieses Konto und Deaktiviert für dieses Konto werden die Konten aufgeführt, die für das einzelne Administratorkonto aktiviert oder deaktiviert sind.

23. Juni 2021

[Zu java8.a12 den Parametern hinzugefügt für Lambda.2](#)

Im Standard AWS Foundational Security Best Practices java8.a12 zu den unterstützten Laufzeiten für das Lambda.2 Steuerelement hinzugefügt.

8. Juni 2021

[Neue Integrationen mit MicroFocus ArcSight und NETSCOUT Cyber Investigator](#)

Integrationen mit MicroFocus ArcSight und NETSCOUT Cyber Investigator hinzugefügt. MicroFocus ArcSight erhält Ergebnisse von Security Hub CSPM. NETSCOUT Cyber Investigator sendet Ergebnisse an Security Hub CSPM.

7. Juni 2021

[Details hinzugefügt für AWSSecurityHubServiceRolePolicy](#)

Der Abschnitt mit verwalteten Richtlinien wurde aktualisiert, um Details für die bestehende verwaltete Richtlinie hinzuzufügen AWSSecurityHubServiceRolePolicy , die von der serviceverknüpften Rolle Security Hub CSPM verwendet wird.

4. Juni 2021

[Neue Integration mit Jira Service Management](#)

Der AWS Service Management Connector für Jira sendet Ergebnisse an Jira und verwendet sie, um Jira-Probleme zu erstellen. Wenn die Jira-Probleme aktualisiert werden, werden auch die entsprechenden Ergebnisse in Security Hub CSPM aktualisiert.

26. Mai 2021

[Die Liste der unterstützten Kontrollen für die Region Asien-Pazifik \(Osaka\) wurde aktualisiert](#)

Der Standard der CIS AWS Foundations und der Payment Card Industry Data Security Standard (PCI DSS) wurden aktualisiert und geben nun an, welche Kontrollen im asiatisch-pazifischen Raum (Osaka) nicht unterstützt werden.

21. Mai 2021

[Neue Integration mit Sysdig Secure für die Cloud](#)

Es wurde eine Integration mit Sysdig Secure für die Cloud hinzugefügt. Die Integration sendet die Ergebnisse an Security Hub CSPM.

14. Mai 2021

[Der Standard „Best Practices“ von AWS Foundational Security wurde um Kontrollen erweitert](#)

Neue Steuerelemente für Amazon API Gateway (APIGateway.2 und APIGateway.3), (CloudTrail.4 und CloudTrail.5), Amazon AWS CloudTrail (EC2.15 und EC2.16), EC2 (ElasticBeanstalk.1 und ElasticBeanstalk.2), (Lambda.4), AWS Elastic Beanstalk Amazon RDS AWS Lambda (RDS.12 — RDS.14), Amazon Redshift (Redshift.7), (.3 und .4) und (WAF.1) hinzugefügt. AWS Secrets Manager SecretsManager AWS WAF

10. Mai 2021

[Aktualisierungen GuardDuty und Amazon RDS-Steuerelemente](#)

Der Schweregrad wurde von GuardDuty.1 und PCI.GuardDuty.1 von Mittel auf Hoch geändert. Ein databaseEngines Parameter wurde hinzugefügt RDS.8.

4. Mai 2021

[Dem ASFF wurden neue Ressourcendetails hinzugefügt](#)

In Resources.Details wurden neue Ressourcendetailobjekte für das EC2 Amazon-Netzwerk ACLs, EC2 Amazon-Subnetze und AWS Elastic Beanstalk Umgebungen hinzugefügt.

3. Mai 2021

[Konsolenfelder hinzugefügt, um Filterwerte für EventBridge Amazon-Regeln bereitzustellen](#)

Die neuen vordefinierten Filtermuster für Security Hub EventBridge CSPM-Regeln bieten Konsolenfelder, mit denen Sie Filterwerte angeben können.

30. April 2021

[Die Integration mit AWS Systems Manager Explorer wurde hinzugefügt und OpsCenter](#)

Security Hub CSPM unterstützt jetzt eine Integration mit Systems Manager Explorer und. OpsCenter Die Integration erhält Ergebnisse von Security Hub CSPM und aktualisiert diese Ergebnisse in Security Hub CSPM.

26. April 2021

[Neuer Typ für Produktintegrationen](#)

Ein neuer Integrationsstyp, UPDATE_FINDINGS_IN_SECURITY_HUB , weist darauf hin, dass eine Produktintegration die Ergebnisse aktualisiert, die sie von Security Hub CSPM erhält.

22. April 2021

[„Hauptkonto“ wurde in „Administratorkonto“ geändert.](#)

Der Begriff „Hauptkonto“ wird in „Administratorkonto“ geändert. Der Begriff wurde auch in der Security Hub CSPM-Konsole und API geändert.

22. April 2021

[APIGateway.1 wurde aktualisiert, um HTTP durch WebSocket zu ersetzen](#)

Titel, Beschreibung und Problembehebung für APIGateway .1 wurden aktualisiert. Das Steuerelement sucht nun nach der Protokollierung der WebSocket-API-Ausführung statt nach der Protokollierung der HTTP-API-Ausführung.

9. April 2021

[GuardDuty Die Amazon-Integration wird jetzt in Peking und Ningxia unterstützt](#)

Die CSPM-Integration mit Security Hub GuardDuty wird jetzt in den Regionen China (Peking) und China (Ningxia) unterstützt.

05. April 2021

[nodejs14.x Zu den unterstützten Laufzeiten für die Lambda.2-Steuerung hinzugefügt](#)

Das Lambda.2-Steuerelement im Standard Foundation Security Best Practices unterstützt jetzt die Laufzeit nodejs14.x

30. März 2021

[Security Hub CSPM im asiatisch-pazifischen Raum \(Osaka\) eröffnet](#)

Security Hub CSPM ist jetzt in der Region Asien-Pazifik (Osaka) verfügbar.

29. März 2021

[Zu den Suchdetails wurden Felder für die Suche nach Anbietern hinzugefügt](#)

Im Bereich „Ergebnisdetails“ enthält der neue Abschnitt „Felder für die Suche nach Anbietern“ die Werte für Zuverlässigkeit, Kritikalität, verwandte Ergebnisse, Schweregrad und Typen.

24. März 2021

[Option hinzugefügt, um sensible Ergebnisse von Amazon Macie zu erhalten](#)

Die Integration mit Macie kann jetzt so konfiguriert werden, dass sensible Ergebnisse an Security Hub CSPM gesendet werden.

23. März 2021

[Umstellung auf die Kontoverwaltung AWS Organizations](#)

Für Kunden, die bereits über ein Administratorkonto mit Mitgliedskonten verfügen, wurden neue Informationen hinzugefügt, wie Sie von der Verwaltung von Konten auf Einladung zur Verwaltung von Konten mithilfe von Organizations wechseln können.

22. März 2021

[Neue Objekte in ASFF für Informationen zur Konfiguration von Amazon S3 Public Access Block](#)

In Resources bietet ein neues Objekt mit `AwsS3AccountPublicAccessBlock` Ressourcentyp und Details Informationen zur Amazon S3 Public Access Block-Konfiguration für Konten. Im Objekt mit den `AwsS3Bucket` Ressourcendetails stellt das `PublicAccessBlockConfiguration` Objekt die Public Access Block-Konfiguration für den S3-Bucket bereit.

18. März 2021

[Neues Objekt in ASFF, mit dem Anbieter gefunden werden können, um bestimmte Felder zu aktualisieren](#)

Das neue FindingProviderFields Objekt in ASFF wird verwendet, BatchImportFindings um Werte für Confidence, Criticality, RelatedFindings, Severity, und bereitzustellen. Types Die ursprünglichen Felder sollten nur mit BatchUpdateFindings aktualisiert werden.

18. März 2021

[Neues DataClassification Objekt für Ressourcen in ASFF](#)

Das neue Resources.DataClassification Objekt in ASFF wird verwendet, um Informationen über sensible Daten bereitzustellen, die auf der Ressource erkannt wurden.

18. März 2021

[CONFIG_RETURNS_NOT_APPLICABLE Mehrwert der verfügbaren Compliance-Statuscodes](#)

Für den NOT_AVAILABLE Konformitätsstatus wurde der Ursachencode entfernt RESOURCE_NO_LONGER_EXISTS und der Ursachencode hinzugefügt CONFIG_RETURNS_NOT_APPLICABLE.

16. März 2021

[Neue verwaltete Richtlinie für die Integration mit AWS Organizations](#)

Eine neue verwaltete Richtlinie, `AWSecurityHubOrganizationsAccess`, gewährt den Organizations die Berechtigungen, die für das Organisationsverwaltungskonto und das delegierte Security Hub CSPM-Administratorkonto erforderlich sind.

15. März 2021

[Informationen zu verwalteten Richtlinien und dienstbezogenen Rollen wurden in das Kapitel Sicherheit verschoben](#)

Die Informationen zu verwalteten Richtlinien wurden überarbeitet und erweitert. Sowohl die Informationen zu verwalteten Richtlinien als auch die Informationen zu dienstbezogenen Rollen wurden in das Kapitel Sicherheit verschoben.

15. März 2021

[Neue Integration mit DB SecureCloud](#)

SecureCloudDB wurde zur Liste der Integrationen von Drittanbietern hinzugefügt. SecureCloudDB ist ein Cloud-natives Datenbanksicherheitstool, das einen umfassenden Überblick über interne und externe Sicherheitslage und -aktivitäten bietet. SecureCloudDB sendet Ergebnisse an Security Hub CSPM.

4. März 2021

[Der Schweregrad der Kontrollen CIS 1.1 und CIS 3.1 — CIS 3.14 wurde überarbeitet](#)

Der Schweregrad der Kontrollen CIS 1.1 und CIS 3.1 — CIS 3.14 wurde auf Niedrig geändert.

3. März 2021

<u>Das Steuerelement RDS.11 wurde entfernt</u>	Das RDS.11-Steuerelement wurde aus dem Standard „Bewährte Methoden für grundlegende Sicherheit“ entfernt.	3. März 2021
<u>Die Integration für Turbot wurde aktualisiert</u>	Die Turbot-Integration wurde aktualisiert, um sowohl Ergebnisse zu senden als auch zu empfangen.	26. Februar 2021
<u>Dem Standard „Bewährte Methoden für grundlegende Sicherheit“ wurden zusätzliche Kontrollen hinzugefügt</u>	Neue Steuerelemente für Amazon API Gateway (APIGateway.1), Amazon EC2 (EC2.9 und EC2.10), Amazon Elastic File System (EFS.2), Amazon OpenSearch Service (ES.2 und ES.3), Elastic Load Balancing (ELB.6) und () (KMS.3) hinzugefügt. AWS Key Management Service AWS KMS	11. Februar 2021
<u>ProductArn Optionaler Filter zur DescribeProducts API hinzugefügt</u>	Die DescribeProducts API-Operation enthält jetzt einen optionalen ProductArn Parameter. Der ProductArn Parameter wird verwendet, um die spezifische Produktintegration zu identifizieren, für die Details zurückgegeben werden sollen.	3. Februar 2021

[Neue Integration mit Antivirus
für Amazon S3 von Cloud
Storage Security](#)

Die Integration mit Antivirus for Amazon S3 sendet die Ergebnisse der Virensuche als Ergebnisse an Security Hub CSPM.

27. Januar 2021

[Das Verfahren zur Berechnung der Sicherheitsbewertung für Administratorkonten wurde aktualisiert](#)

Für ein Administratorkonto verwendet Security Hub CSPM einen separaten Prozess zur Berechnung der Sicherheitsbewertung. Das neue Verfahren stellt sicher, dass die Bewertung Kontrollen umfasst, die für Mitgliedskonten aktiviert, für das Administratorkonto jedoch deaktiviert sind.

21. Januar 2021

[Neue Felder und Objekte im ASFF](#)

Es wurde ein neues Action Objekt hinzugefügt, um Aktionen zu verfolgen, die gegen eine Ressource aufgetreten sind. Dem AwsEc2NetworkInterface Objekt wurden Felder hinzugefügt, um DNS-Namen und IP-Adressen zu verfolgen. Den Ressourcendetails wurde ein neues AwsSsmPatchCompliance Objekt hinzugefügt.

21. Januar 2021

[Dem Standard „Best Practices für grundlegende Sicherheit“ wurden Kontrollen hinzugefügt](#)

Neue Steuerelemente für Amazon CloudFront (CloudFront.1 bis CloudFront.4), Amazon DynamoDB (DynamoDB.1 bis DynamoDB.3), Elastic Load Balancing (ELB.3 bis ELB.5), Amazon RDS (RDS.9 bis RDS.11), Amazon Redshift (Redshift.1 bis Redshift.3 und Redshift.6) und Amazon SNS (SNS.1) hinzugefügt.

15. Januar 2021

[Der Workflow-Status wird basierend auf dem Datensatzstatus oder dem Compliance-Status zurückgesetzt](#)

Security Hub CSPM setzt den Workflow-Status automatisch von NOTIFIED oder RESOLVED auf zurück, NEW wenn ein archiviertes Ergebnis aktiviert wird oder wenn sich der Compliance-Status eines Befundes von entweder PASSED auf FAILED, WARNING oder ändert. NOT_AVAILABLE Diese Änderungen deuten darauf hin, dass zusätzliche Untersuchungen erforderlich sind.

7. Januar 2021

[Es wurden ProductFields Informationen für Ergebnisse hinzugefügt, die auf Kontrollen basieren](#)

Für Ergebnisse, die anhand von Kontrollen generiert wurden, wurden Informationen über den Inhalt des ProductFields Objekts im AWS Security Finding Format (ASFF) hinzugefügt.

29. Dezember 2020

[Aktualisierungen der verwalteten Erkenntnisse](#)

Der Titel von Insight 5 wurde geändert. Es wurde ein neuer Insight (32) hinzugefügt, der nach IAM-Benutzern mit verdächtigen Aktivitäten sucht.

22. Dezember 2020

[Aktualisierungen der IAM.7- und Lambda.1-Steuerregeln](#)

Im Standard AWS Foundational Security Best Practices wurden die Parameter für IAM.7 aktualisiert. Der Titel und die Beschreibung von Lambda.1 wurden aktualisiert.

22. Dezember 2020

[Erweiterte Integration mit ITSM ServiceNow](#)

Die ServiceNow ITSM-Integration ermöglicht es Benutzern, automatisch Vorfälle oder Probleme zu erstellen, wenn ein Security Hub CSPM-Ergebnis eingeht. Aktualisierungen dieser Vorfälle oder Probleme führen zu Aktualisierungen der Ergebnisse in Security Hub CSPM.

11. Dezember 2020

[Neue Integration mit AWS Audit Manager](#)

Security Hub CSPM bietet jetzt eine Integration mit AWS Audit Manager. Die Integration ermöglicht es Audit Manager, kontrollbasierte Ergebnisse von Security Hub CSPM zu erhalten.

08. Dezember 2020

[Neue Integration mit Aqua Security Kube-Bench](#)

Security Hub CSPM hat eine Integration mit Aqua Security Kube-Bench hinzugefügt. Die Integration sendet die Ergebnisse an Security Hub CSPM.

24. November 2020

[Cloud Custodian ist jetzt in den Regionen China verfügbar](#)

Die Integration mit Cloud Custodian ist jetzt in den Regionen China (Peking) und China (Ningxia) verfügbar.

24. November 2020

[BatchImportFindings kann jetzt verwendet werden, um zusätzliche Felder zu aktualisieren](#)

Bisher konnten Sie die Types `FelderConfidence` , `Criticality` `RelatedFindings` `Severity`, und nicht `BatchImportFindings` zum Aktualisieren verwenden . Wenn diese Felder nicht von `aktualisiert wurdenBatchUpdateFindings` , können sie nun von `aktualisiert werdenBatchImportFindings` . Sobald sie von `aktualisiert wurdenBatchUpdateFindings` , können sie nicht mehr von `aktualisiert werdenBatchImportFindings` .

24. November 2020

[Security Hub CSPM ist jetzt integriert in AWS Organisationen](#)

Kunden können jetzt Mitgliedskonten mithilfe ihrer Organisationskontokonfiguration verwalten. Das Organisationsverwaltungskonto bestimmt das Security Hub CSPM-Administratorkonto, das festlegt, welche Organisationskonten in Security Hub CSPM aktiviert werden sollen. Der manuelle Einladungsprozess kann weiterhin für Konten verwendet werden, die nicht Teil einer Organisation sind.

23. November 2020

[Das separate Suchlistenformat für Steuerelemente mit hohem Volumen wurde entfernt](#)

Die Ergebnisliste für ein Steuerelement verwendet nicht mehr das Seitenformat „Ergebnisse“, wenn es eine sehr große Anzahl von Ergebnissen gibt.

19. November 2020

[Neue und aktualisierte Integrationen von Drittanbietern](#)

Security Hub CSPM unterstützt jetzt Integrationen mit cloudtamer.io, 3CORESec, Prowler und Kubernetes Security. StackRox IBM sendet keine Ergebnisse mehr. QRadar Es empfängt nur Ergebnisse.

30. Oktober 2020

[Option zum Herunterladen der Ergebnisliste von der Kontrolldetailseite hinzugefügt.](#)

Auf der Seite mit den Kontrolldetails gibt es eine neue Download-Option, mit der Sie die Ergebnisliste in eine CSV-Datei herunterladen können. Die heruntergeladene Liste berücksichtigt alle Filter, die in der Liste enthalten sind. Wenn Sie bestimmte Ergebnisse ausgewählt haben, enthält die heruntergeladene Liste nur diese Ergebnisse.

26. Oktober 2020

[Option zum Herunterladen der Liste der Steuerelemente von der Standarddetailseite hinzugefügt.](#)

Auf der Standarddetailseite können Sie mit einer neuen Download-Option die Kontrollliste in eine CSV-Datei herunterladen. Die heruntergeladene Liste berücksichtigt alle Filter, die in der Liste enthalten sind. Wenn Sie ein bestimmtes Steuerelement ausgewählt haben, enthält die heruntergeladene Liste nur dieses Steuerelement.

26. Oktober 2020

Neue und aktualisierte Partnerintegrationen

Security Hub CSPM ist jetzt integriert. ThreatModeler
Die folgenden Partnerintegrationen wurden aktualisiert, um ihren neuen Produktnamen Rechnung zu tragen.
Twistlock Enterprise Edition heißt jetzt Palo Alto Networks - Prisma Cloud Compute.
Demisto, ebenfalls von Palo Alto Networks, ist jetzt Cortex XSOAR und Redlock ist jetzt Prisma Cloud Enterprise.

23. Oktober 2020

Security Hub CSPM in China (Peking) und China (Ningxia) eröffnet

Security Hub CSPM ist jetzt in den Regionen China (Peking) und China (Ningxia) verfügbar.

21. Oktober 2020

Überarbeitetes Format für ASFF-Attribute und Integrationen von Drittanbietern

Die Listen der [ASFF-Attribute](#) und [Partnerintegrationen](#) verwenden jetzt ein listenbasiertes Format anstelle von Tabellen. Die ASFF-Syntax, die Attribute und die Taxonomie der Typen sind jetzt in separaten Themen zusammengefasst.

15. Oktober 2020

Die Standard-Detailseite wurde neu gestaltet

Auf der Standarddetailseite für einen aktivierten Standard wird jetzt eine Liste mit Steuerelementen im Registerformat angezeigt. Die Registerkarten filtern die Kontrollliste auf der Grundlage des Kontrollstatus.

7. Oktober 2020

CloudWatch Ereigniss e wurden ersetzt durch EventBridge	Verweise auf Amazon CloudWatch Events wurden durch Amazon ersetzt EventBridge.	1. Oktober 2020
Neue Integrationen mit Blue Hexagon for AWS, Alcide KAudit und Palo Alto Networks VM-Series.	Security Hub CSPM ist jetzt in Blue Hexagon for AWS, Alcide KAudit und Palo Alto Networks VM-Series integrier t. Blue Hexagon for AWS und KAudit senden die Ergebniss e an Security Hub CSPM. VM- Series erhält Ergebnisse von Security Hub CSPM.	30. September 2020
Neue und aktualisierte Objekte mit Ressourcendetails in ASFF	Neue Resources.Details Objekte fürAwsApiGat ewayRestApi , AwsApiGatewayStage ,AwsApiGatewayV2Api ,AwsApiGatewayV2Sta ge ,AwsCertif icateManagerCertif icate AwsElbLoa dBalancer AwsIamGro up , und AwsRedshi ftCluster hinzugefü gt. Es wurden Details zu den AwsIamAccessKey ObjektenAwsCloudF rontDistribution , AwsIamRole und hinzugefü gt.	30. September 2020

[Neues ResourceRole Attribut für Ressourcen in ASFF, um zu verfolgen, ob es sich bei einer Ressource um einen Akteur oder ein Ziel handelt.](#)

Das ResourceRole Attribut für Ressourcen gibt an, ob die Ressource das Ziel der Suchaktivität oder der Täter der Findungsaktivität ist. Die gültigen Werte sind ACTOR und TARGET.

30. September 2020

[AWS Systems Manager Patch Manager wurde zu den verfügbaren AWS Serviceintegrationen hinzugefügt](#)

AWS Systems Manager Patch Manager ist jetzt in Security Hub CSPM integriert. Patch Manager sendet Ergebnisse an Security Hub CSPM, wenn Instances in der Flotte eines Kunden nicht mehr dem Patch-Compliance-Standard entsprechen.

22. September 2020

[Der Standard „Bewährte Methoden für AWS grundlegende Sicherheit“ wurde um neue Kontrollen erweitert](#)

Neue Steuerelemente für die folgenden Dienste hinzugefügt: Amazon EC2 (EC2.7 und EC2 .8), Amazon EMR (EMR.1), IAM (IAM.8), Amazon RDS (RDS.4 bis RDS.8), Amazon S3 (S3.6) und (.1 und .2). AWS Secrets Manager SecretsManager

15. September 2020

[Neue Kontextschlüssel BatchUpdateFindings für die IAM-Richtlinie zur Steuerung des Zugriffs auf Felder](#)

IAM-Richtlinien können jetzt so konfiguriert werden, dass der Zugriff auf Felder und Feldwerte bei der Verwendung eingeschränkt wird. BatchUpdateFindings

10. September 2020

Erweiterter Zugriff auf BatchUpdateFindings für Mitgliedskonten	Standardmäßig haben Mitgliedskonten jetzt denselben Zugriff BatchUpdateFindings wie Administratorkonten.	10. September 2020
Neue Kontrollen AWS KMS im Foundational Security Best Practices Standard	Zwei neue Kontrollen (KMS.1 und KMS.2) wurden dem Foundational Security Best Practices Standard hinzugefügt. Die neuen Kontrollen prüfen, ob IAM-Richtlinien den Zugriff auf Entschlüsselungsaktionen einschränken. AWS KMS	9. September 2020
Die Ergebnisse für Kontrollen auf Kontoebene wurden entfernt	Security Hub CSPM generiert keine Ergebnisse mehr auf Kontoebene für eine Kontrolle. Es werden nur Ergebnisse auf Ressourcenebene generiert.	1. September 2020
Neues PatchSummary Objekt in ASFF	Das PatchSummary Objekt wurde der ASFF hinzugefügt. Das PatchSummary Objekt stellt Informationen zur Patch-Konformität einer Ressource im Verhältnis zu einem ausgewählten Konformitätsstandard bereit.	1. September 2020

[Die Seite mit den Kontrolldetails wurde neu gestaltet](#)

Die Detailseite für Steuerelemente wurde neu gestaltet. Die Liste mit den Ergebnissen von Kontrollen enthält Registerkarten, mit denen Sie die Liste schnell nach dem Konformitätsstatus filtern können. Sie können auch schnell unterdrückte Ergebnisse einsehen. Jeder Eintrag bietet Zugriff auf zusätzliche Details zur Suchressource, zur AWS Config Suchregel und zu Suchnotizen.

28. August 2020

[Neue Filteroptionen für Ergebnisse](#)

Für die Suche nach Filtern können Sie den Filter `ist nicht` verwenden, um Ergebnisse zu finden, bei denen ein Feldwert nicht dem Filterwert entspricht. Sie können den Befehl `„Beginnt nicht mit“` verwenden, um nach Ergebnissen zu suchen, bei denen ein Feldwert nicht mit dem angegebenen Filterwert beginnt.

28. August 2020

[Neue Objekte mit Ressourcendetails in ASFF](#)

Neue Resources
 .Details Objekte für die folgenden Ressourcentypen hinzugefügt: AwsDynamoDbTable, AwsEc2Eip, „AwsIamPolicy“, „AwsIamUser“, „AwsRdsDbCluster“, „AwsRdsDbClusterSnapshot“, „AwsRdsDbSnapshot“, „AwsSecretsManagerSecret“.

18. August 2020

[Neue Integration mit RSA Archer](#)

Security Hub CSPM ist jetzt in RSA Archer integriert. RSA Archer erhält Ergebnisse von Security Hub CSPM.

18. August 2020

[Neues Beschreibungsfeld für AwsKmsKey](#)

Dem AwsKmsKey Objekt unter wurde ein Description Feld hinzugefügt. `gtResources.Details`.

18. August 2020

[Es wurden Felder hinzugefügt zu AwsRdsDbInstance](#)

Dem AwsRdsDbInstance Objekt unter wurden mehrere Attribute hinzugefügt. `gtResources.Details`.

18. August 2020

[Die Art und Weise, wie Security Hub CSPM den Gesamtstatus einer Kontrolle bestimmt, wurde aktualisiert](#)

Bei Kontrollen, für die keine Ergebnisse vorliegen, lautet der Status Keine Daten statt Unbekannt. Der Kontrollstatus umfasst sowohl Ergebnisse auf Konto- als auch auf Ressourcenebene. Der Kontrollstatus verwendet nicht den Workflow-Status von Ergebnissen, es sei denn, unterdrückte Ergebnisse werden ignoriert.

13. August 2020

[Die Art und Weise, wie Security Hub CSPM die Sicherheitsbewertung für einen Standard berechnet, wurde aktualisiert](#)

Bei der Berechnung der Sicherheitsbewertung für einen Standard ignoriert Security Hub CSPM jetzt Kontrollen mit dem Status Keine Daten. Die Sicherheitsbewertung ist das Verhältnis der bestandenen Kontrollen zu den aktivierten Kontrollen, ausgenommen Kontrollen ohne Daten.

13. August 2020

[Neue Option zur automatischen Aktivierung neuer Kontrollen in aktivierten Standards](#)

Es wurde eine Einstellungsoption hinzugefügt, um neue Steuerelemente in aktivierten Standards automatisch zu aktivieren. Sie können diese Option auch mithilfe der UpdateSecurityHubConfiguration API-Operation konfigurieren.

31. Juli 2020

Neue Kontrollen für den Payment Card Industry Data Security Standard (PCI DSS)

Dem PCI DSS-Standard wurden neue Steuerungen hinzugefügt. Die Bezeichner der neuen Steuerelemente lauten PCI.DMS.1, PCI. EC21.5, PCI. EC2.6, PCI. ELBV2.1, PCI. GuardDuty .1, PCI.IAM.7, PCI.IAM.8 , PCI.S3.5, PCI.S3.6, PCI. SageMaker.1, PCI.SSM.2 und PCI.SSM.3.

29. Juli 2020

Neue und aktualisierte Kontrollen für den Standard Foundational Security Best Practices

Dem Standard „Best Practices“ von Foundational Security wurden neue Kontrollen hinzugefügt. Die Bezeichner der neuen Steuerelemente lauten AutoScaling .1, DMS.1, EC2 .4, EC2 .6, S3.5 und SSM.3. Der Titel von ACM.1 wurde aktualisiert und der Wert des Parameters auf 30 geändert. daysToExpiration

29. Juli 2020

Neues Vulnerabilities Objekt in der ASFF

Das Vulnerabilities Objekt wurde hinzugefügt, das Informationen über Sicherheitslücken bereitstellt, die mit dem Befund in Verbindung stehen.

1. Juli 2020

Neue Resource.Details Objekte in ASFF for Auto Scaling: Gruppen, EC2 Volumes und EC2 VPCs	Die AwsEc2Vpc Objekte AwsAutoSc alingAutoScalingGr oup AWSEc2Volume , und wurden hinzugefügt. Resource.Details	1. Juli 2020
Neues NetworkPath Objekt in der ASFF	Das NetworkPath Objekt wurde hinzugefügt, das Informationen über einen Netzwerkpfad bereitstellt, der mit dem Ergebnis zusammenh ängt.	1. Juli 2020
Ergebnisse automatisch auflösen, Complianc e.Status wenn PASSED	Falls dies der Fall Complianc e.Status istPASSED, setzt Workflow.Status Security Hub CSPM bei Ergebnissen aus Kontrollen automatisch auf. RESOLVED	24. Juni 2020
AWS Command Line Interface Beispiele	AWS CLI Syntax und Beispiele für mehrere Security Hub CSPM-Aufgaben hinzugefü gt. Beinhaltet die Aktivieru ng von Security Hub CSPM, die Verwaltung von Erkenntni ssen, die Verwaltung von Standards und Kontrollen, die Verwaltung von Produktin tegrationen und die Deaktivie rung von Security Hub CSPM.	24. Juni 2020

[Neues Attribut im ASFF
Severity.Original](#)

Das Attribut Severity.Original wurde hinzugefügt, wobei es sich um den ursprünglichen Schweregrad des Ergebnisanbieters handelt. Dies ersetzt das veraltete Severity.Product -Attribut.

20. Mai 2020

[Neues Compliance.StatusReasons Objekt
im ASFF für Details zum
Status eines Steuerelements](#)

Es wurde das Objekt Compliance.StatusReasons hinzugefügt, das zusätzlichen Kontext für den aktuellen Status einer Kontrolle bereitstellt.

20. Mai 2020

[Neuer AWS grundlegender Standard für bewährte
Sicherheitsverfahren](#)

Der neue Standard „Bewährte Methoden für AWS grundlegende Sicherheitsverfahren“ wurde hinzugefügt. Dabei handelt es sich um eine Reihe von Kontrollen, die erkennen, wann Ihre bereitgestellten Konten und Ressourcen von den bewährten Sicherheitsmethoden abweichen.

22. April 2020

[Neue Konsolenoption zum
Aktualisieren des Workflow-
Status für ein Ergebnis](#)

Es wurden Informationen zur Verwendung der Security Hub-Konsole oder -API hinzugefügt, um den Workflow-Status für Ergebnisse festzulegen.

16. April 2020

[Neue BatchUpdateFindings API für Kundenaktualisierungen von Ergebnissen](#)

Es wurden Informationen zur Verwendung von BatchUpdateFindings hinzugefügt, um Informationen im Zusammenhang mit dem Prozess der Untersuchung eines Ergebnisses zu aktualisieren. BatchUpdateFindings ersetzt UpdateFindings, das veraltet ist.

16. April 2020

[Aktualisierungen des AWS Security Finding Format \(ASFF\)](#)

Mehrere neue Ressourcentypen hinzugefügt. Dem Severity-Objekt wurde ein neues Label-Attribut hinzugefügt. Label soll das Normalized -Feld ersetzen. Es wurde ein neues Workflow-Objekt hinzugefügt, um den Prozess einer Untersuchung zu einem Ergebnis zu verfolgen. Workflow enthält ein Status-Attribut, das das vorhandene Workflows Tate -Attribut ersetzt.

12. März 2020

[Aktualisierungen der Seite „Integrationen“](#)

Aktualisiert, um die Änderungen an der Integrationsseite anzuzeigen. Für jede Integration zeigt die Seite nun die Integrationskategorie und ob jede Integration Ergebnisse an Security Hub CSPM sendet oder Ergebnisse von Security Hub CSPM empfängt. Sie enthält auch die spezifischen Schritte, die erforderlich sind, um jede Integration zu ermöglichen.

26. Februar 2020

[Neue Integrationen von Drittanbieterprodukten](#)

Die folgenden neuen Produktintegrationen wurden hinzugefügt: Cloud Custodian, FireEye Helix, Forcepoint CASB, Forcepoint DLP, Forcepoint NGFW, Rackspace Cloud Native Security und Vectra.ai Cognito Detect.

21. Februar 2020

[Neuer Sicherheitsstandard für den Payment Card Industry Data Security Standard \(PCI DSS\)](#)

Der Security Hub CSPM-Sicherheitsstandard für den Payment Card Industry Data Security Standard (PCI DSS) wurde hinzugefügt. Wenn dieser Standard aktiviert ist, führt Security Hub CSPM automatisierte Prüfungen anhand von Kontrollen durch, die sich auf die PCI DSS-Anforderungen beziehen.

13. Februar 2020

[Aktualisierungen des AWS Security Finding Format \(ASFF\)](#)

Ein Feld für [zugehörige Anforderungen für Standardkontrollen](#) wurde hinzugefügt. [Neue Ressourcentypen und neue Ressourcendetails](#) wurden hinzugefügt. Mit dem ASFF können Sie jetzt bis zu 32 Ressourcen bereitstellen.

5. Februar 2020

[Neue Option zum Deaktivieren einzelner Sicherheitsstandardskontrollen](#)

Es wurden Informationen hinzugefügt, wie Sie steuern können, ob jedes einzelne Sicherheitsstandard-Steuererelement aktiviert ist.

15. Januar 2020

[Aktualisierungen der Security Hub CSPM-Konzepte](#)

Einige Beschreibungen wurden aktualisiert und den [Security Hub CSPM-Konzepten](#) neue Begriffe hinzugefügt.

21. September 2019

[AWS Allgemeine Verfügbarkeit von Security Hub Cloud Security Posture Management \(CSPM\)](#)

Inhaltsaktualisierungen, um den Verbesserungen Rechnung zu tragen, die während der Betaphase an Security Hub CSPM vorgenommen wurden.

25. Juni 2019

[Es wurden Schritte zur Problembehebung für CIS Foundations-Prüfungen hinzugefügt AWS](#)

Es wurden Korrekturschritte zu den [Sicherheitsstandards](#) hinzugefügt, die in [AWS Security Hub Cloud Security Posture Management \(CSPM\)](#) [unterstützt](#) werden.

15. April 2019

[Betaversion von AWS Security
Hub Cloud Security Posture
Management \(CSPM\)](#)

Hat die Beta-Version des AWS
Security Hub Cloud Security
Posture Management (CSPM)
-Benutzerhandbuchs veröffent
licht.

18. November 2018

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.